Open Architecture (OA) Computing Environment Technologies and Standards

Version 1.0

23 August 2004

Prepared for:

PROGRAM EXECUTIVE OFFICE, INTEGRATED WARFARE SYSTEMS
Program Manager, Open Architecture (OA)
1333 Isaac Hull Avenue SE
Washington Navy Yard, DC 20376-2301

Prepared by:

Naval Surface Warfare Center Dahlgren Division (NSWCDD)
17320 Dahlgren Road
Dahlgren, VA 22448-5100

OACE Tech & Stds 1.0
23 August 2004

Open Architecture Program: An Enterprise Approach to Introducing Open Architecture Into Navy Warfare Systems…and Beyond

"Statement A: Document approved for Public Release: Distribution is unlimited."

FOREWORD

The Assistant Secretary of the Navy for Research, Development and Acquisition (ASN (RDA)) assigned the Program Executive Office for Integrated Warfare Systems (PEO IWS) with responsibility for coordinating the introduction of open architectures into the Navy's warfare systems. The Open Architecture (OA) initiative is a multi-faceted strategy providing a framework for developing Joint interoperable systems that adapt and exploit open-system design principles and architectures.

The strategy calls, in part, for establishment of OA Computing Environments (OACE) through the dissemination of guidance and standards that describe types of computing systems that will exploit open system design principles. The initial implementation guidance for OA addresses a family of hardware and software standards as well as guidance on developing software based warfighting functions that will perform well in an extensible architecture. The extensible characteristics of these types of open architectures will permit the use and implementation of a wide variety of products, including reusable software components, requirements analysis, contract language, process descriptions, test cases and scenarios, models, simulations, designs and architectures and human expertise across Naval Air, Land, and Undersea platforms. This initial implementation reflects a shift in focus from a platform-centered warfare system development approach to a more integrated, Battle Force (BF)-centered approach.

The introduction of open architectures into Naval Warfare Systems will be formally instituted through the Open Architecture Enterprise Team (OAET) established by ASN RDA in August of 2004. However, this OA documentation is intended for use in the surface ship combat systems domain and has been released by PEO IWS. In the future, all documentation related to the OA initiative will be released by the OAET. The OACE Technologies and Standards document (this document) provides a core set of technologies and standards that apply to the OACE technology base. The OACE Design Guidance document provides guidance concerning design aspects of the standards-based computing environment that is to be used in OA warfighting systems.

EXECUTIVE SUMMARY

Computing technology is a key part of the OA effort. A unified standards-based set of computing resources that is to be used in OA warfighting systems is called the Open Architecture Computing Environment (OACE). This document provides a core set of technologies and standards that apply to the OACE technology base. A companion document, *Open Architecture Computing Environment Design Guidance [reference a]*, provides guidance concerning design aspects of the standards-based computing environment that is to be used in OA warfighting systems.

This document is intended to provide overall guidance for the design and implementation of warfighting-capable software that, when coupled with OACE, will meet mission requirements for Naval warfighting systems. Initial review indicates that the design guidance as written has applicability in both the warfighting system domain and the Command, Control, Communication, Computers, and Intelligence (C4I) domains. Therefore, it is anticipated that parts of the guidance are extensible to selected C4I systems, the specifics of which are left to the system developers and government program offices.

This document contains three major technical sections. The first, Section 4, OACE Technology Base, discusses the OACE technologies by technology area emphasizing issues that impact standards for that technology area. The second, Section 5, Standards and OACE Compliance, enumerates mandated and emerging standards by technology area. The third, Section 6, OACE Compliance Assessment, describes how to document OACE compliance claims.

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

Section **Page**

ILLUSTRATIONS

Figure **Page**

TABLES

Table **Page**

SECTION 1

INTRODUCTION

1.1 PURPOSE

The purpose of this document is to define the computing technology base and standards that are to be used in OA warfighting systems. The overall set of computing resources used in OA systems is called the Open Architecture Computing Environment (OACE). This document describes the initial OACE technologies, identifies the standards used in defining the initial OACE, and defines compliance assessment to these OACE standards.

Achieving commonality of warfighting components across Naval Warfare systems places a corresponding requirement for application computer program portability across potentially differing equipment and support software bases. The rapidly changing nature of Commercial Off-the-Shelf (COTS) software also levies portability requirements on application software as an enabler of low-cost COTS technology refreshes.

To that end, the OA initiative includes a coherent computing technology strategy based on the widely employed commercial practice called ***open systems***—that is, non-proprietary, standards-based systems that are easy to upgrade and change over time. This strategy is based on maximum use of a compatible set of layered, standards-based computing technologies, many of them real-time capable. Such real-time capabilities have processing constraints that are coupled to physics-based system requirements. Within this layered approach, various forms of adaptive and service-based third-party software, collectively called ***middleware***, provide additional isolation mechanisms between applications and equipment that contribute to application portability.

1.2 SCOPE

This document applies to the computing implementation of the functional capabilities embodied in naval warfare systems, including but not limited to the warfare systems noted below. The OA Enterprise Team established by ASN(RDA) in August of 2004, will expand the applicability of this document, over time.

a. Aegis-equipped cruisers and destroyers (DDG new construction and CG/DDG backfit)

b. Ship Self Defense System (SSDS)-equipped carriers and large deck amphibious assault ships (e.g., LPDs and LHDs [new construction and backfit])

c. Submarines (new construction and backfit)

d. DD(X) land attack destroyer (future construction)

e. Littoral Combat Ship (LCS) (future construction)

f. E-2C and other tactical aircraft's mission payloads (new construction and backfit)

1.2.1 Computational Domain Applicability

The scope to which OACE capabilities apply encompasses most but not all combat system and support system application areas. Included are:

a. Real-time tactical computation requirements that can be met by mainstream commercial products.

b. Physically embedded computational requirements that can be met by well-accepted niche market products.

c. Tactical display and decision support requirements that can be met by mainstream COTS.

d. High-security requirements that can be met by appropriate commercial technology, albeit niche market.

Not included within the present scope of OACE are performance domains for which custom-designed special purpose devices are required to meet performance requirements. Also not included are decision support resources with little or no real-time requirements and other systems such as:

a. Extremely high performance domains (e.g., some signal processing).

b. Low-level embedded devices such as those that implement machinery control or other Hull, Mechanical and Electrical (HM&E) functions.

c. Command support functions such as those associated with Information Technology – 21st Century (IT-21).

d. Administrative or personal computing support (e.g., personal laptops).

In the case of IT-21, further examination is required to determine the degree of overlap between IT-21 and OACE. In any case, interconnect and bridging technologies for interfacing components of the above types to OACE-based systems are included.

1.3 TECHNICAL APPROACH

OACE computing infrastructure components provide the computational framework upon which both common and unique warfighting and support applications are to be built under the guidelines of the OA Enterprise Team initiative. The overall scope of OACE includes technical architecture, standards and products. Conceptually, OACE provides isolation of warfighting applications and services by means of a standards-based, layered approach (Figure 1-1). As shown, the OACE uses Resource Management (RM) technology to adjust computing allocations to available resources, however, specific approaches to RM are not dictated in this document. RM technology is described in Section 4.11.

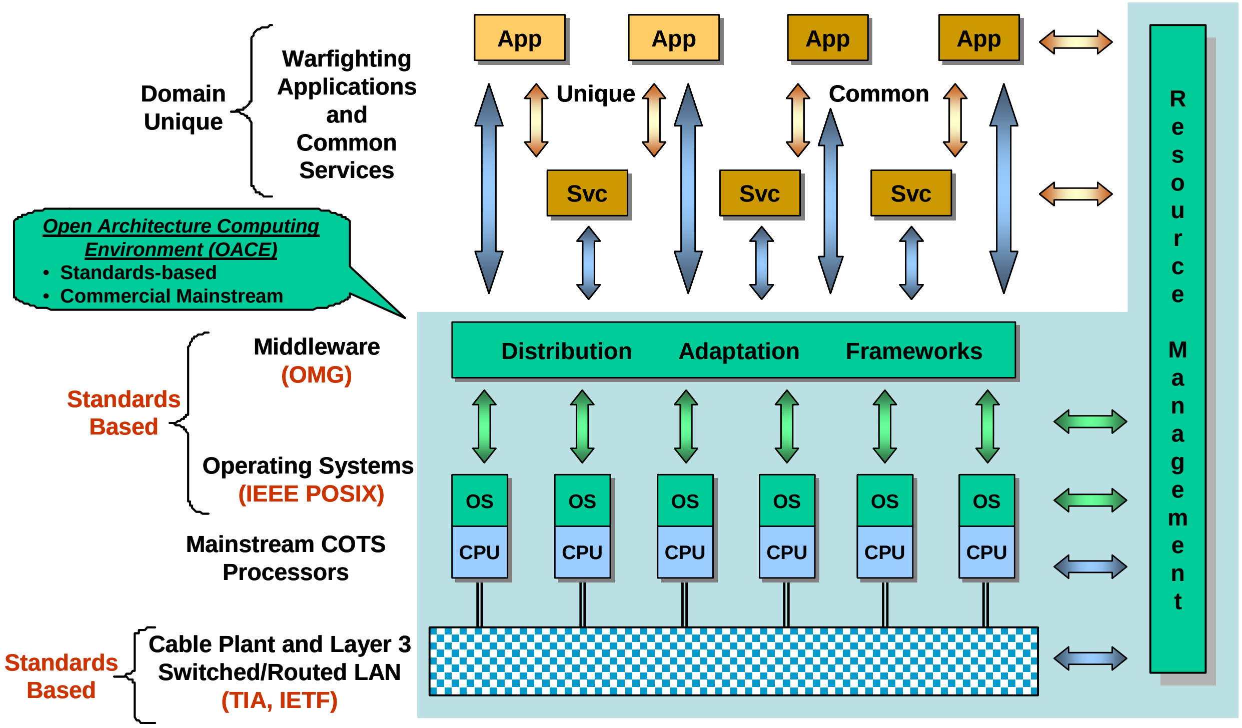


Figure 1-1. Open Architecture Layered Approach

The description of the OACE technology set is based on a reference architecture that is applicable to mission-critical distributed systems. The reference architecture, discussed in Section 3.2, is a representation of the key technologies (and their interrelationships) known to be suitable for successful development and fielding of Navy warfighting systems. Requirements encompass various aspects of real-time computation as well as various support requirements (e.g., display, decision support and security).

This document describes each of the OACE technologies and identifies the standards that they are based on. Where standards do not yet exist, the approach for implementing the functions of the OACE technology is provided.

1.3.1 Open Systems

The OA initiative and its computing environment, the OACE, are based on the widespread commercial practice called open systems. The open approach has been widely adopted because open systems convey certain benefits in terms of reduced life-cycle cost, reduced time-to-market, increased ability to interoperate and cooperate with others, and reduced personnel training. A number of open-systems definitions exist within the literature. From a process and business strategy point of view, this document adopts the definition provided by the Open Systems Joint Task Force (OSJTF), which operates at the level of the Office of the Secretary of Defense (OSD):

> ***"An Open Systems Approach is*** *an integrated business and technical strategy that employs a modular design and, where appropriate, defines key interfaces using widely supported, consensus-based standards that are published and maintained by a recognized industrial standards organization."* [reference b]

A number of technical definitions for open systems are available. Given the selection of standards for OA, perhaps one of the most relevant is the definition adopted for the POSIX operating system standard by IEEE.

> **Open system:** *"A system that implements sufficient open specifications or standards for interfaces, services, and supporting formats to enable properly engineered application software:*
>
> - *To be ported with minimal changes across a wide range of systems from one or more suppliers*
> - *To interoperate with other applications on local and remote systems*
> - *To interact with people in a style that facilitates user portability*" [reference c]

1.3.2 Computing Standards

A major goal of the open approach to computing chosen for OA is to enable the development of applications that are portable across multiple brands and generations of COTS computing products. This portability is fostered primarily through 1) choice of computing products that conform to widely accepted commercial standards (wherever possible), and 2) through the use of middleware for communications, abstraction of services, and Application Programmer Interfaces (APIs). Thus, standards are a cornerstone of the open-systems approach.

The standards chosen for use in OA are described in this document. They are drawn from a number of widely respected standards communities and are compatible with the standards identified in the *Department of Defense (DoD) Joint Technical Architecture (JTA)* [reference d] as described in Section 5. These standards include:

a. Telecommunications Industry Association (TIA) – physical media (e.g., fiber optics)

b. Internet Engineering Task Force (IETF) – networks and protocols

c. IEEE POSIX – operating systems

d. Object Management Group (OMG) – distribution middleware (e.g., Common Object Request Broker Architecture [CORBA] and Data Distribution Service (DDS])

e. International Organization for Standardization (ISO) – Ada programming language (the use of which is restricted to legacy applications) and Structured Query Language (SQL) for information management

f. American National Standards Institute (ANSI) – C++ language

g. Java Community Process – Java programming language and infrastructure, Java Data Objects (JDO) and Java Database Connectivity (JDBC) information management

1.3.3 Product Selection

This document defines the technologies and standards applicable to OACE infrastructure components, no further product selection guidance is within the scope of this document.

1.3.4 Federated vs. Integrated

It should be acknowledged that the OA goal of commonality is, to some degree, in tension with the goal of providing maximum flexibility of choice to acquisition managers. For developing functional application programs, the term ***integrated*** is used to describe the system-wide commonality approach, and the term ***federated*** is used to describe a contrasting approach where choice is unrestricted. An instantiation of the OACE will need to support the approach used.

The integrated approach enables mission flexibility and enhanced failure recovery through a high degree of redundancy delivered via operational resource sharing. It may also engender economies of scale in procurement, although this is less important in an era of very low-cost COTS processors. The federated approach allows maximum flexibility to meet stressing or system-unique requirements through selection of leading-edge technologies. It also places fewer requirements on programs to align their schedules with factors outside their immediate programs.

Neither federation nor integration is preferred in the specification of OA. Both approaches are supported by OACE standards, thus allowing program managers to adopt a system approach that is best suited to their developmental and operational requirements. In either case, the benefits of OA can be attained.

One of the means by which commonality is encouraged is the availability of on-line management of computing resources. This capability, similar to the ***total ship computing*** utilized in the *DD-21 Operational Requirements Document* [reference e], permits resource sharing, mission optimization and failure recovery on a ship-wide basis across all compatible computing resources. This service is available to all systems that are able to participate in the integrated approach, but it does not preclude employment of the federated approach for systems that have requirements that justify a different approach.

1.3.5 OACE Change Management

Errata for this document are maintained at: https://viewnet.nswc.navy.mil

Current mainstream COTS computing technology meets many, but not all warfighting computing requirements. However, the pace of computing technology innovation has been very rapid for decades and shows little signs of slackening. Thus, in the future mainstream products may meet many requirements that currently are met only by special purpose solutions. Because of this rapid evolution, the boundaries between what is within OACE scope and what is not will require periodic reconsideration.

For this reason, an OACE change management process will be formally documented in the future through the Open Architecture Enterprise Team (OAET) established by ASN RDA August 2004. This formal process will provide for periodic review of the standards contained in this document. This change process, cyclic in nature, will include mechanisms for incorporating the requirements of each program manager as well as inputs from industry.

1.4 DOCUMENT OVERVIEW

Section 2 provides applicable documents identified within the main body of this document (excluding the Standards Listings). Section 3 provides a list of the OACE Technology Areas, introduces the OACE Reference Architecture, identifies the primary standards bodies for the OACE Technology Areas, describes the OACE Compliance Categories, and describes processor pooling. Section 4 discusses the OACE Technologies by Technology Area, emphasizing issues that impact standards for each area. Section 5 provides the compliance statements of mandated and emerging standards by Technology Area. Section 6 discusses OACE compliance assessments.

SECTION 2

APPLICABLE DOCUMENTS

a. *Open Architecture Computing Environment Design Guidance*, Version 1.0; dated 23 August 2004.

b. *An Open System Approach to Weapon System Acquisition*, Version 1.0, Working Draft; http://www.acq.osd.mil/osjtf/approach/approach_os.html.

c. IEEE Std 1003.0-1995; *IEEE Guide to the POSIX Open System Environment (OSE)*.

d. *DoD Joint Technical Architecture (JTA)*, Version 6.0, Volumes 1 and 2, dated 3 October 2003. Future OACE standards documentation releases will reference the DoD Information Technology Standards and Profile Registry (DISR) that is currently evolving from the JTA.

e. *DD-21 Operation Requirements Document (ORD)*.

f. IEEE Std 1003.1-2003; IEEE *Standard for Information Technology - Portable Operating System Interface (POSIX)* - Base Definitions.

g. IEEE Std 1003.13-2003; *IEEE Standard for Information Technology - Standardized Application Environment Profile - POSIX® - Realtime Application Support*.

h. *Updated Data Distribution Service Final Adopted Specification*; dated 7 July 2003; http://www.omg.org/docs/ptc/03-07-07.pdf.

i. Department of Defense Directive Number 8500.1; dated October 24, 2002; http://www.dtic.mil/whs/directives/corres/pdf/d85001_102402/d85001p.pdf.

j. *Navy Recommended Fiber Optic Components Parts List*; dated 21 May 2003.

SECTION 3

TECHNOLOGY OVERVIEW

The OACE technology base consists of a number of computing technologies. In aggregate, these technologies largely reflect the current state of the practice as it applies to real-time systems and other associated systems of a tactical Navy nature. Wide ranges of computing technologies are available in addition to those listed herein. However, only technologies that can deliver the real-time performance needed by weapon systems or that provide capabilities needed for these weapon systems are included in the OACE technology base.

Other technology domains, such as those applicable to business or web applications, are briefly discussed but not included in this version of this document. If deemed appropriate, they may be discussed in a future version. Periodically, individual technologies will be reviewed, using a process currently under development (as described in Section 1.3.5), for possible future inclusion as their apparent viability merits.

3.1 OACE TECHNOLOGIES

The following list constitutes the set of technologies considered under the scope of OACE. This document provides the OA compliance requirements for these technologies.

a. Physical Media

b. Enclosures

c. Information Transfer

d. Computing Resources

e. Operating Systems

    1. General Purpose
    2. Real-Time

f. Peripherals

g. Adaptive Middleware

h. Distribution Middleware

    1. Distributed Object Computing
    2. Publish-Subscribe Protocols
    3. Group Ordered Communication Protocols
    4. Data Parallel

i. Frameworks

j. Information Management

k. Resource Management

l. Security Services

   1. Commercial Best Practice
   2. Data Separation

m. Time Synchronization

n. Programming Languages

3.2 TECHNOLOGY BASE COMPONENT RELATIONSHIPS

Figure 3-1 provides an abstracted view of a number of the technology base components and their interrelationships. This diagram contains the OACE technology base components. The diagram is notional in nature and does not necessarily imply a particular design or implementation. For example, three of the classes of Distribution Middleware listed in Section 3.1 (i.e., Distributed Objects, Group-Ordered, and Publish-Subscribe) appear as separate components in the reference architecture. However, the future evolution of the OMG-distributed computing standards is in the direction of providing the three key distribution middleware protocols within a single product family.

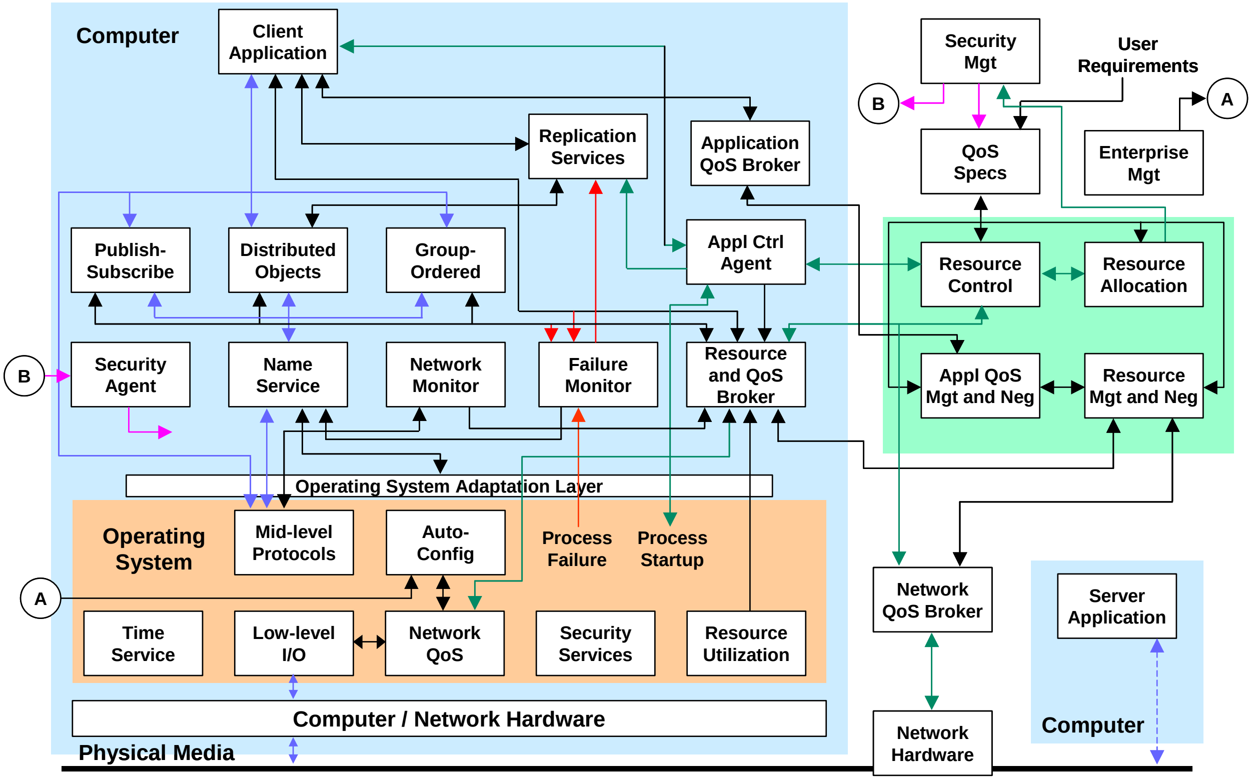


Figure 3-1. OACE Technology Base Component Relationships

3.3 SOURCES OF STANDARDS

Table 3-1 below provides initial information as to the source of standards for those components for which standards have been selected.

Table 3-1. Sources of OACE Standards

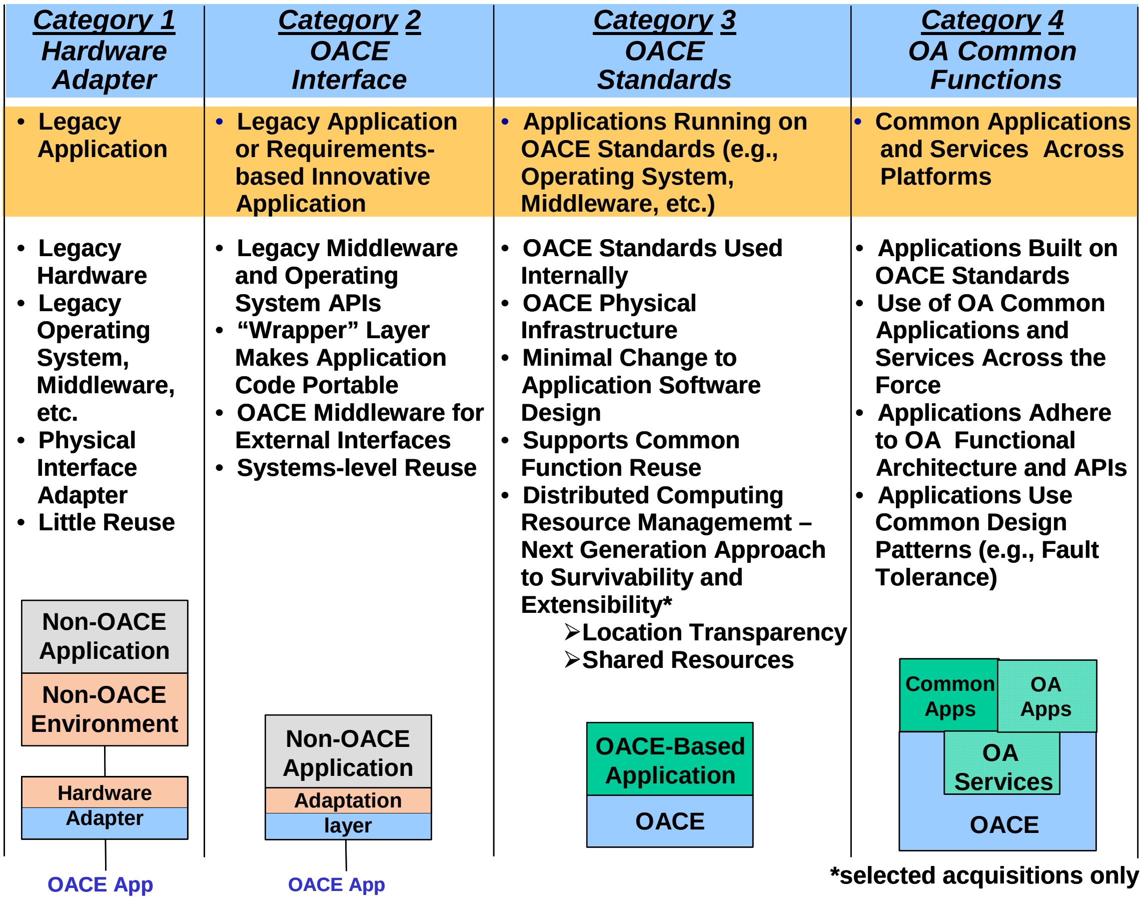
TECHNOLOGY COMPONENT	SOURCE OF STANDARD
Physical Media	MIL standards, Commercial Item Description (CID), Electronics Industry Association (EIA)/ TIA
Enclosures	None at present
Information Transfer	IETF, IEEE, JTA

Table 3-1. Sources of OACE Standards (Continued)

TECHNOLOGY COMPONENT	SOURCE OF STANDARD
Computing Resources	Commercial products of various types
Operating Systems	IEEE POSIX standard, JTA
Peripherals	Various
Adaptive Middleware	POSIX-based
Distribution Middleware	OMG standard for CORBA and DDS, Message-Passing Interface (MPI) Forum, World Wide Web Consortium (W3C)
Frameworks	None at present
Information Management	ISO, Java Community Process (JCP)
Resource Management	None at present
Security Services	National Institute of Standards and Technology (NIST), IETF, JTA
Time Synchronization	Inter-Range Instrumentation Group (IRIG), IETF Network Time Protocol (NTP), JTA
Programming Languages	ISO, ANSI, JCP

3.4 OACE COMPLIANCE CATEGORIES

There are four approaches identified for tactical systems to work with/within an OACE infrastructure. Figure 3-2 shows the four approaches. OACE compliance is defined for three of these categories; two are defined as the Fully OACE Compliant categories and the other is the OACE Interface category. OACE compliance assessments referenced against this document are required to identify a particular Fully OACE Compliant category or the OACE Interface category.



Category 1 ***Hardware Adapter***	***Category 2*** ***OACE Interface***	***Category 3*** ***OACE Standards***	***Category 4*** ***OA Common Functions***
• Legacy Application	• Legacy Application or Requirements-based Innovative Application	• Applications Running on OACE Standards (e.g., Operating System, Middleware, etc.)	• Common Applications and Services Across Platforms
• Legacy Hardware • Legacy Operating System, Middleware, etc. • Physical Interface Adapter • Little Reuse	• Legacy Middleware and Operating System APIs • "Wrapper" Layer Makes Application Code Portable • OACE Middleware for External Interfaces • Systems-level Reuse	• OACE Standards Used Internally • OACE Physical Infrastructure • Minimal Change to Application Software Design • Supports Common Function Reuse • Distributed Computing Resource Managememt – Next Generation Approach to Survivability and Extensibility* ➢Location Transparency ➢Shared Resources	• Applications Built on OACE Standards • Use of OA Common Applications and Services Across the Force • Applications Adhere to OA Functional Architecture and APIs • Applications Use Common Design Patterns (e.g., Fault Tolerance)

*selected acquisitions only

Figure 3-2. OACE Compliance Categories

A Hardware Adapter (Category 1) approach applies to a legacy system not built to the OACE standards interfaced to OACE-based applications via a hardware adapter that is compliant with the OACE standards identified in this document. The only compliance issues are with the hardware adapter and not with the legacy system. OACE compliance assessments are not used with this approach.

An OACE Interface (Category 2) approach uses an Adaptation Layer that isolates a legacy application program(s) (based on non-OACE infrastructure components) from an OACE infrastructure. The Adaptation Layer should provide Operating System wrapper functions, design pattern components, and system interfaces for use by non-OACE applications. OACE compliant middleware is used for all communications with OACE-compliant application programs. Legacy distribution middleware (i.e., non-OACE) may be used within the application programs ported using this approach. Such middleware may be used between legacy application programs and is not used to pass information with an OACE-compliant application program. Because legacy middleware may introduce complexities in the reuse of an application program (or its constituent components), it should be periodically examined for replacement by OACE-compliant middleware. OACE Interface compliance is achieved by providing the necessary capabilities for the non-OACE application to communicate with OACE application programs using OACE distribution middleware standards.

OACE Standards (Category 3) is an OACE fully compliant approach that uses an OACE-compliant infrastructure but does not use OA Common Services and OA Common Functions. While the use of OA Common Services and OA Common Functions are not required, the use/reuse of this type of software is enabled given the underlying OACE infrastructure. For this approach, legacy applications are typically ported to OACE infrastructures. In such a port, minimal changes are made to the application architecture. Distributed Computing RM is an option for selected acquisitions by which a great degree of survivability and extensibility is provided by the use of location independence and a sharing of computing resources. Distributed Computing Resource Management is at an early stage of development (e.g., standardization efforts have begun and prototypes have been demonstrated) that may be applicable at this time for new construction acquisitions. It is expected that in the future when Distributed Computing Resource Management standards are developed, they will be considered for incorporation into the OACE standards set.

OA Common Functions (Category 4) is an OACE fully compliant approach that uses an OACE-compliant infrastructure for which application programs have been designed to use the OA architectural patterns/frameworks (e.g., OA fault tolerance pattern) where applicable. Such applications must use the OA Common Services (e.g., time synchronization, navigation and data extraction/reduction [DX/DR]) and OA Common Functions versus different (e.g., legacy) approaches for such services and functions when these are needed. Such applications need to be developed with planned periodical upgrades as new OA infrastructure capabilities, OA Common Services and OA Common Functions become available.

3.5 POOLS OF PROCESSING

As previously described, one of the focus areas for the OACE infrastructure is to support an integrated software approach. In such an approach, a program would deliver a module of application software (using the OA Common Services and Functions) instead of delivering a unique set of hardware and infrastructure software bundled with a system’s unique application software. In the integrated software approach, the module of application software delivered would run with a variety of other applications on a common pool of processors within an OACE infrastructure. Aboard a platform there may be a number of such pools of processors, as shown in Figure 3-3. Each pool would host a number of integrated software applications with compatible security requirements and operating characteristics.

Both of the Fully OACE Compliant categories support running application software upon a pool of processors. The opposite extreme would be a Hardware Adapter (Category 1) approach using a hardware adapter to isolate a legacy system from an OACE pool (or pools) of processors.

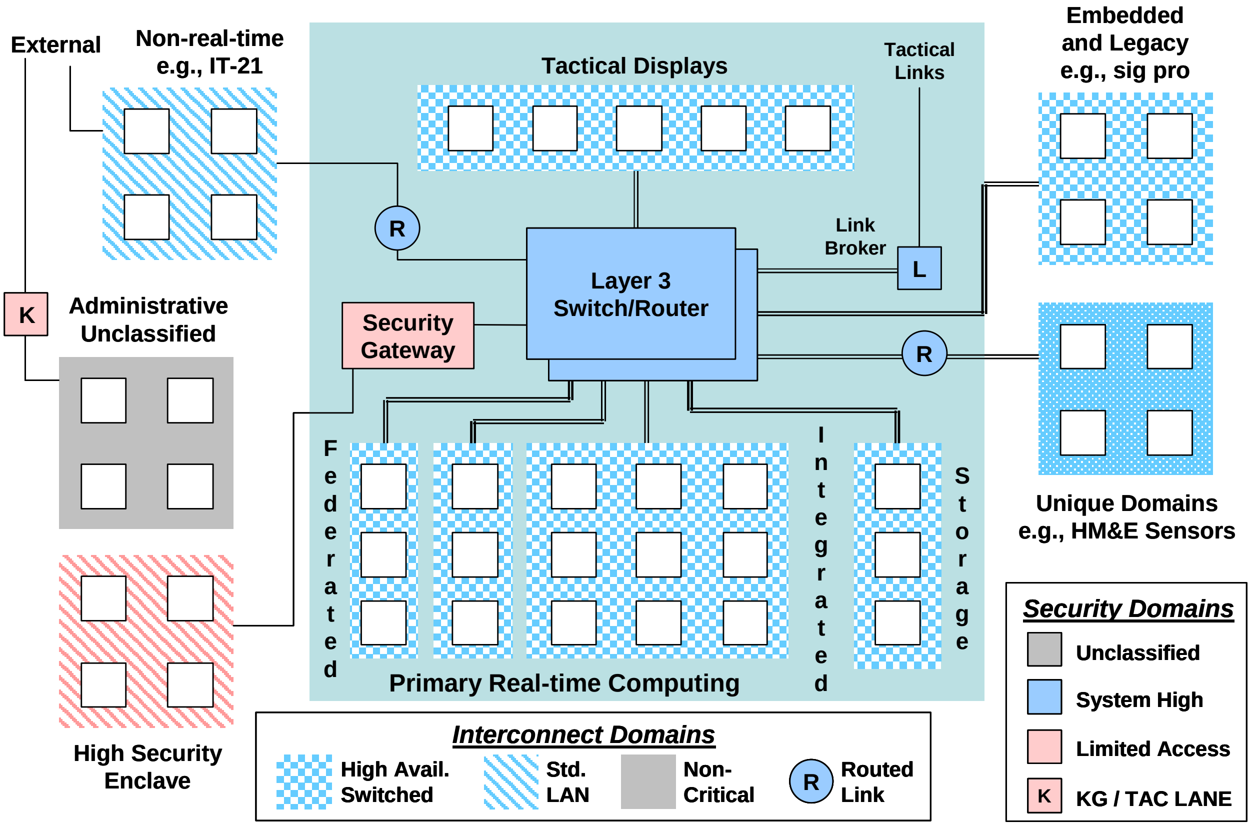


Figure 3-3. Notional Pools of Computing Aboard a Tactical Platform

OACE compliance statements provided within this document can be tied to the characteristics of the pools of processors provided for the applications. For example, a compliance statement may allow a pool of processors to utilize a choice of one of two Operating System alternatives, which are currently identified as OACE compliant.

SECTION 4

OACE TECHNOLOGY BASE

4.1 PHYSICAL MEDIA

Physical media products/components are used to develop the cable topology installed aboard naval platforms. The OA Physical Media standards and specifications provide for design and installation standards as well as both military-unique and commodity COTS-based product specifications. Military performance specifications are developed for Navy-unique products used in applications where environmental or safety requirements (e.g., low-smoke, zero halogens) are to be met. Commercial Item Descriptions (CIDs) are developed for commodity COTS-based products to ensure interoperability among products. These standards and specifications are used to reduce the long-term risk of the shipboard cable topology.

There are many military and commercial physical media technologies available that address the Navy's physical media goals of Open Architecture. These technologies can be placed in several categories:

a. <u>Optical Fiber</u>: A filament-shaped waveguide made of dielectric material, such as glass or plastic, that guides light. It usually consists of a single, discrete, optically transparent transmission element consisting of at least a cylindrical core with cladding on the outside.

1. <u>Multimode Fiber</u>: An optical fiber that allows more than one mode to propagate at a given wavelength. The number of modes depends on the core diameter, numerical aperture, and wavelength.
2. <u>Single Mode Fiber</u>: An optical fiber in which only one bound mode can propagate at a given wavelength and numerical aperture.

b. <u>Optical Fiber Cable</u>: A cable in which one or more optical fibers are used as the propagation medium.

1. <u>Blown Optical Fiber (BOF) Cable</u>: A cable that contains one or more BOF tubes through which optical fibers or optical fiber bundles are blown.
2. <u>Conventional Optical Fiber Cable</u>: An optical fiber cable in which the optical fiber is an integral part of the cable and is installed during the cable manufacturing process.

c. <u>Single Terminus Connectors</u>: In fiber optics, a connector that is designed and intended from use inside of an interconnection box (distribution box) or cabinet.

d. <u>Multi-Terminus Heavy Duty Connectors</u>: In fiber optics, a connector that is designed and intended from use outside of an interconnection box (distribution box) or cabinet.

e. Optical Fiber Terminus: A device used to terminate an optical fiber, which provides a means of locating and holding the fiber within a connector.

f. Interconnection Box: A housing for holding fiber optic splices, connectors, couplers, and BOF tubes used to distribute signals on incoming cables to outgoing cables by means of connections.

g. BOF Components: Components used for installing, interconnecting, and terminating BOF tubes and fibers.

h. Twisted Pair (TP) Cable: Electrical cable with 100 ohm TP and an optimized braided shield and outer jacket; used for Local Area Networks (LANs).

i. TP Connectors: A device used to terminate TP cable, which provides a means of locating and holding the electrical conductors.

Baseline specifications for these products are currently in place.

The physical media products must meet the specific environmental requirements and the installation applications for which they are targeted. There are multiple vendors across these product lines that have been qualified or approved to the Navy's specifications, and these products are currently being used in the Fleet. However, the physical media technology is an ever-changing market, and new vendors and new product offerings are ongoing. There are new products for which specifications are being developed and new products that are at various levels of maturity.

4.2 ENCLOSURES

Enclosures are used to mount COTS equipment aboard naval platforms. The standard for many years has been the 19"-wide rack. COTS products to be mounted in enclosures include computers, peripherals, and network switches. Example products include a large number of commercial racks without environmental isolation, as well as the Q70 Embedded Processor Subsystem (EPS) rack and the Aegis Mission Critical Enclosure (MCE) cabinet.

COTS equipment enclosures (19" racks) are readily obtainable in a variety of heights and depths. The key issue is whether the enclosure itself provides any environmental isolation (e.g., shock and vibration) for the COTS equipment or whether this isolation is provided via other means.

If a programmatic decision is made to use a common set of enclosures, then the following issues will need to be addressed:

a. Specify the enclosure environmental isolation required.

b. How will equipment suites be tested for environmental isolation?

c. Will changing equipment in the enclosure require retesting?

4.3 INFORMATION TRANSFER

The Information Transfer Technologies and Standards fall into three broad categories: Connectivity Protocols, Transfer Protocols, and Support Protocols. These protocols are used in varying combinations as required in specific OACE products. Examples of OACE products that require Information Transfer Standards include computers (network interface cards), operating systems (the IP Protocol Suite), Enterprise Class Layer 2/3 switches, access routers, Enterprise Network Management, and Wireless Access Points.

The Connectivity Protocols are the lower layer protocols that are included in the ISO Open System Interconnection (OSI) Reference Model's Physical and Data Link layers. They provide basic physical and logical connectivity between communicating devices. The most common family of standards in this category is the IEEE 802 Local Area Network Standards, including various types of Ethernet.

The Transfer Protocols are the middle layer protocols that are included in the ISO OSI Reference Model's Network and Transport layers. They provide end-to-end data transfer over potentially multiple types of network connectivity protocols. The Internet Protocol (IP) is the single common denominator for providing end-to-end interoperability. All of the protocols required to provide this end-to-end transfer are provided here, including routing protocols and basic quality-of-service (QoS) functionality.

Finally, the Support Protocols are the upper layer protocols that are included in the ISO OSI Reference Model's Session, Presentation, and Application layers. This group of protocols provides common communication services, including file transfer and e-mail transfer. Wide ranges of protocols exist in this category, representing a wealth of functionality.

4.4 COMPUTING RESOURCES

Computing resources as described here include all general purpose or dynamically reconfigurable computing devices required to support the OACE with the one exception of tactical display processors, which will come from the current programs such as the Q70 or future Navy-defined display processing efforts. Examples include personal computers (PCs); common commercial UNIX workstations; symmetric multiprocessor servers and a wide variety of single board computers (SBCs), many of them designed for the Virtual Microbus European (VME) backplane chassis standard.

Middleware techniques are viewed as isolating the application software from changes at the computer hardware (and operating system) technology level, but the following are factors to minimize the number of types of computers within OACE:

a. Performance qualification of computing hardware can be a cost driver. Many different items are often bundled with the computing hardware (e.g., operating systems, time synchronization software, and network interfaces). Typically, performance can only be measured given specific hardware and software. Thus, if OA has a large set of critical performance measures (e.g., time synchronization capabilities of **X** microseconds), then qualifying a computer to all of the performance requirements may be expensive. Selecting a common set of computing hardware may reduce duplicative qualification efforts and, thus, reduce costs.

b. Environmental qualification of computers may be a cost driver. A common set of computers may minimize such testing.

c. Life-cycle costing and logistic/maintenance issues may force the number of processor types down to a minimum.

Although it would be easier to manage the entire set of computing resources on a platform as homogeneous computing resources, two factors make it an unreasonable expectation:

a. Different applications require a different mix of hardware support—some are Input/Output (I/O) intensive, some are compute intensive, some are memory intensive—which indicates that a heterogeneous mix of computing resources might better support the computational needs of the ship.

b. Some applications require real-time support. A requirement for homogeneity will force all applications to run in a real-time environment. This places a heavy burden on software developers because real-time systems tend to be less portable and, due to a much smaller market share, lag the development of the wider software development world.

A goal is to support heterogeneity *transparently* through a layered architecture and an adaptive RM capability. This will allow each individual tactical computing environment to continually evolve through small, incremental, discrete purchasing decisions as the applications themselves evolve to better support the needs of the tactical environment.

4.5 OPERATING SYSTEMS

In today's computing systems, it is becoming increasingly important to design software with operating systems that are based on widely recognized industry standards. This is even more important for systems designed for longevity, where the hardware and software infrastructure will change during the system's life cycle. Standards are pervasive in today's systems, and new standards are constantly being defined to address the rapidly changing state of technology.

To be effective, a standard must be based on established technology and widely accepted by industry. The POSIX family of standards includes over 30 individual standards. First published in 1990, POSIX defines a standard for application portability across different operating system platforms. The original POSIX 1003.1a defines standard interfaces to such core functions as file operations, process management, signals, and devices. Later releases have been defined to address such topics as real-time extensions (1003.1b, d, j and 1003.21) and threading (1003.1c).

Functions defined in the original real-time extension standard 1003.1b (process functions) and 1003.1c (thread functions) are supported across a large number of operating systems. Specific features defined in POSIX 1003.1b include the following:

a. Periodic Timers

b. Priority Scheduling: fixed priority preemptive scheduling with a minimum of 32 priority levels

c. Real-time Signals with Multiple Levels of Priority

d. Semaphores: named and memory counting semaphores

e. Message Passing: message passing using named queues, optionally priority ordered

f. Shared Memory: named memory regions shared between multiple processes

g. Memory Locking: functions to prevent swapping of physical pages

h. Asynchronous I/O: allows non-blocking device reads and writes.

Commercial support for POSIX varies. To be POSIX conformant requires certification testing of the operating system and hardware platform to a suite of tests. POSIX is established as a set of optional features; this allows vendors to implement portions of the POSIX standards while remaining POSIX compliant. Compliance within the POSIX community requires only that vendors provide a compliance document that lists options supported and configuration limits imposed. OACE requirements for POSIX compliance are provided in Section 5.5.

The core of the Open Group Single UNIX Specification, Version 3, is also ANSI/IEEE Std 1003.1-2003, [reference f] which is also known as the ISO/IEC 9945-1:2003 standard. ANSI/IEEE Std 1003.1-2003 is a major revision that incorporates ANSI/IEEE Std 1003.1-1990 (POSIX.1) and all of its subsequent amendments as well as ANSI/IEEE Std 1003.2-1992 (POSIX.2) and its subsequent amendments and is combined with the core volumes of the Single UNIX Specification, Version 2. It is technically identical to *The Open Group, Base Specifications, Issue 6*; they are one and the same document, the front cover having both designations. This document will henceforth refer to this specification as the IEEE 1003-2003.1 standard.

4.5.1 Real-time Support

An operating system is just one component of any system that includes hardware, application software, other system software (e.g., middleware), and possibly a network or interconnection infrastructure. In a system containing elements that must respond to stimuli within a certain amount of time (i.e., having real-time requirements), the insertion of a real-time operating system (RTOS) addresses only one element in a complex system, albeit a critically important element. An RTOS alone, while essential for application and system predictability, cannot compensate for insufficient predictability in the remaining system elements. As a chain is merely as strong as its weakest link, so system predictability is limited by the predictability of its least predictable element.

The POSIX standard promotes portability of applications; however, in real-time systems, predictability and low overhead are important. Historically, portability has often been sacrificed to meet predictability requirements. Embedded real-time systems usually have space and resource restrictions that may make full compliance with all aspects of POSIX inappropriate. The POSIX 1003.13 profile standard [reference g] establishes four profiles for systems based on four levels of system functionality. Table 4-1 shows a high level overview of these current real-time POSIX profiles:

Table 4-1. POSIX 1003.13 Profiles

PROFILE	*NUMBER OF PROCESSES*	*THREADS*	*FILE SYSTEMS*
54	Multiple	Yes	Yes
53	Multiple	Yes	Simple
52	Single	Yes	Simple
51	Single	Yes	No

4.6 PERIPHERALS

The OA peripherals include both Man Machine Interface peripherals and I/O peripherals. The list of peripherals identified for OA include:

a. Man Machine Interface Peripherals

1. Keyboard
2. Mouse
3. Cathode Ray Tube (CRT) Display

4. Liquid Crystal Display (LCD)
5. Plasma Display
6. Speaker

b. I/O Peripherals

1. Hard Drive
2. Compact Disk (CD) Read/Write
3. Digital Video Disk (DVD) Read/Write
4. Printer
5. Raid Mass Storage Device
6. Network Attached Storage (NAS) peripherals
7. Storage Area Network (SAN)
8. Digital Linear Tape Backup Storage/Retrieval Devices

4.7 ADAPTIVE MIDDLEWARE

Adaptive middleware technology isolates applications from the differences in operating systems and compilers, thus increasing portability. Although standards for both operating system (e.g., POSIX) and compilers (e.g., C++) exist, in practice varying degrees of compliance with specific versions of the standards can affect the ability to readily port software between products produced by different vendors.

Adaptive middleware is available via widely used open-source products, commercial vendors and through products developed by DoD contractors. Adaptive middleware products are targeted for a particular language, such as C++. Although there are no specific standards for adaptive middleware, products are generally based on the POSIX family of operating system standards. The use of adaptive middleware is understood to be a long-term undertaking on the part of OA.

Unfortunately, the different adaptation middleware implementations are not fully interchangeable. Thus, a decision to use a particular adaptive middleware product would thereafter preclude the use of another without (possibly extensive) source code porting. For this reason, if an adaptive middleware product is selected for use, it is preferable that the product isolate and encapsulate the necessary operating system functionality and provide wide usage across multiple platforms. An important consideration for adaptation middleware is whether the middleware package itself is open source—that is, the source code for the middleware itself is available for developers to maintain the use of the middleware product for as long a time as possible. This provides longer viability of the application until the need arises to migrate the application already written from one middleware standard/product to another one.

As an alternative to adaptive middleware, it is possible to obtain complete adaptive environments, such as allowing a Microsoft environment to appear like a standards-compliant POSIX environment. However, few vendors sell these products; furthermore, these products offer little support for real-time applications.

4.8 DISTRIBUTION MIDDLEWARE

Four types of distribution middleware are discussed, including distributed objects, publish-subscribe protocols, group-ordered communication protocols, and message-passing middleware for data parallel applications. Additionally, as it is recognized that occasionally the need may exist to have interactions between components developed using different middleware standards and/or products, bridging between middleware products is discussed.

4.8.1 Introduction to Multiple Distribution Middleware Standards and Families

Computing technology innovation continues at a rapid pace. Thus, while standards exist within the overall computing community, the rapid pace of innovation means that standards themselves will evolve, albeit at a slower pace than the technologies they address. Furthermore, new standards appear and old standards disappear. For this reason, it is important to define a framework within which standards-based products may evolve and change over time. This phenomenon is a significant driver in devising systematic approaches to legacy capture and transition.

In addition, many widely divergent communities use computing products, ranging from business automation to real-time control systems. Because of this situation, multiple families of standards exist, and for each one there is a recognized domain of applicability. For this reason, it is necessary in selecting standards to specify to what problem space a particular standard is applied.

In the area of distribution middleware, several families of standards have evolved to meet the needs of a wide variety of user domains. Depending on use, each has a greater or lesser domain of applicability and therefore, an inherent market share. Among the more likely families of standards for distribution middleware, both *de jure* (formal international standards body) and *de facto* (dominant vendor and/or large market share), the following distributed object models stand out as possibilities for OA application:

a. Distributed Component Object Model (DCOM): Large market share distributed object technology driven almost exclusively by Microsoft; serves as de facto standard for business and non-real-time decision analysis such as those that might be associated with mission planning.

b. Java/Remote Method Invocation (RMI): Large market share distributed object technology driven primarily by Sun Microsystems but maintained by a separate standards organization; broadly applicable to soft real-time display, human systems integration, and decision aids, as well as to business and other non-real-time applications.

c. CORBA: Formal distributed object standard maintained by OMG; suitable for soft real-time command and control, hard real-time sensor control and weapons control.

d. Data Distribution Service (DDS): Emerging real-time, data-centric, publish-subscribe standard for data distribution developed and driven by the Object Management Group; highly applicable for periodic transmission of hard real-time sensory and weapons data, as well as soft real-time command and control data.

e. MPI: Formal message-oriented standard for low latency message-based communication narrowly used for signal processing and other extremely low latency data parallel processes.

These product families and their most prominent domains of applicability are represented graphically in Figure 4-1.

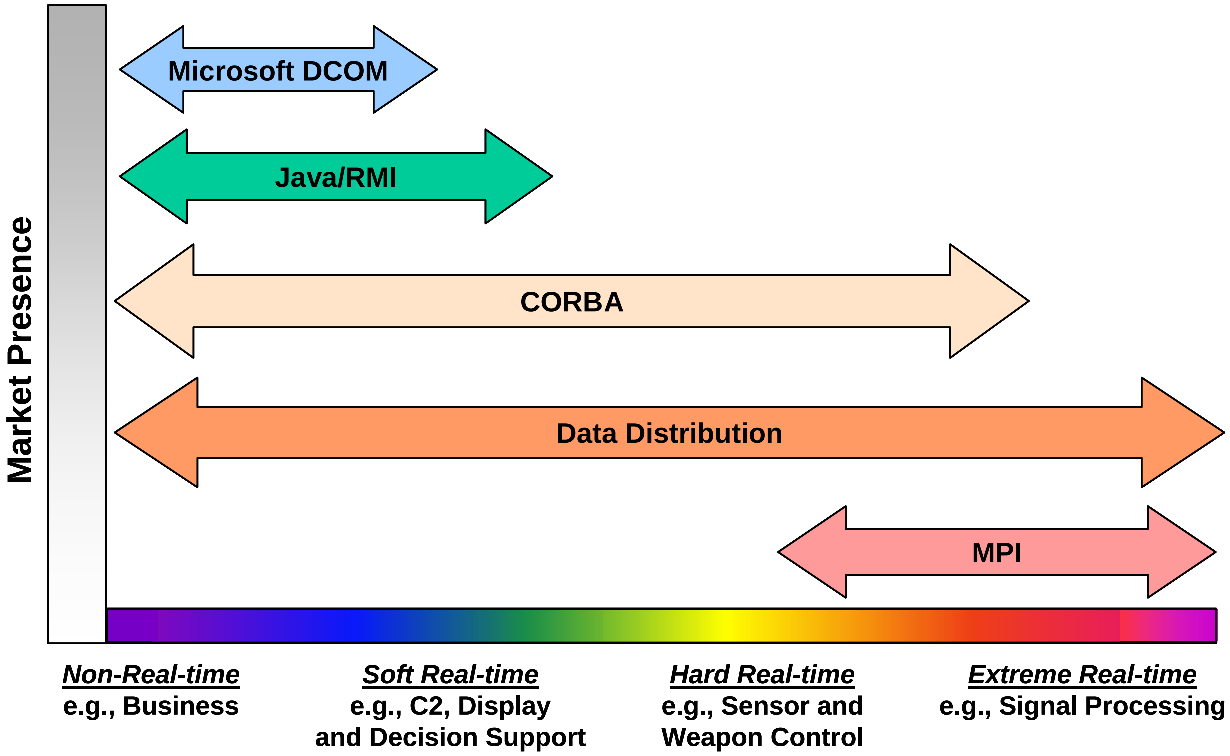


Figure 4-1. Families of Distribution Middleware

Given the likelihood that products adhering to multiple families of standards may appear in OA systems and that the standards themselves may change over time, it is important to identify methods by which these differences may be systematically addressed and to identify appropriate standards within the evolving versions of this OACE standards document. One such method is the use of bridges between products, a method that is widely used in some standards communities.

A key factor in making this strategy work is the selection of standards families that serve as ***integration technologies*** (i.e., those that support integration of disparate products) rather than those that are ***displacement technologies*** (i.e., those that displace other products). Products of the latter type force everything in a system to conform to their model, an approach that is far too restrictive to serve as the basis for a program as broad as OA.

For the four families of products given above, Table 4-2 provides information concerning the current state of the art in bridging between these product families.

Table 4-2. Standards Bridging Technologies

	DCOM	***JAVA/RMI***	***CORBA***	***DATA DISTRIBUTION***	***MPI***
DCOM	DCOM				
Java/RMI	Limited products available	RMI			
CORBA	Multiple products available	Supported by OMG CORBA-Java Language Mapping Spec. Multiple products available.	Internet Inter-ORB Protocol (IIOP) – OMG Standard.		
DDS	No products available. Not likely to be required.	No products available. CORBA-based products may support.	CORBA-based products likely to support.	Product interoperability not currently planned. CORBA-based products may support.	
MPI	No products available. Not likely to be required.	No products available. Not likely to be required.	No products available – OMG CORBA Data Parallel Spec may obviate need.	No products available. Not likely to be required	MPI messages

4.8.2 Distributed Objects

Multiple different distributed object protocols are currently in use. These protocols allow the exchange of information by invoking methods on objects that may reside at some other location on a network. The most widely used examples of distributed object protocols include the CORBA, Microsoft DCOM, and Java/RMI. Of these, only CORBA is a formal standard that is platform neutral, has interfaces available across multiple computer languages, and is supported by a vendor neutral industry consortium. Although a standards process supports Java RMI, it is specific to the Java language. Microsoft DCOM is specific to Microsoft platforms.

The CORBA standard is managed by an active industry standards group of approximately 800 members—the OMG. Extensions to the core standard provide for interoperability of products from different vendors, real-time support, fault tolerance, transactions, object registration and discovery, event notification, and many other features.

The OMG also manages other important technology standards such as the Unified Modeling Language (UML) and the emerging Model Driven Architecture (MDA) standard. Since MDA is intended to support the concept of automatic code generation from UML models, the potential for substantial software productivity and reliability gains is high.

CORBA products that support the major languages of interest to OA (including C++, Java, and Ada) are available. Multiple products are available that are compliant with the CORBA real-time specification.

4.8.3 Publish-Subscribe

Publish-subscribe middleware provides an important middleware capability by supporting the distribution of potentially high-volume, low-latency data from anonymous servers to anonymous clients. Publish-subscribe middleware is widely used to support the development of systems that are highly extensible. Data distributed by a publish-subscribe middleware can be accessed by any application that declares itself a subscriber, thus making it easy to add new functionality without requiring the addition of new interfaces.

The OMG recently adopted the specification for the real-time Data Distribution Service (DDS) [reference h]. The first DDS specification was finalized in early 2004 and will be published as a formal publish-subscribe standard in the near future.

4.8.4 Group-Ordered Communication

Middleware support for building replicated, distributed applications is critical for an OACE. Group communications middleware provides effective support for building such applications. This is accomplished by providing higher levels of delivery guarantees, ordering messages to help with maintaining consistency of state between replicated applications, and detecting and handling communications failures that are ordered with respect to the message flows. The latter feature enables applications to determine which communications activities were completed prior to a failure event or the start up of a new replica.

The most widely used group communications product is arguably Ensemble, developed by Cornell University. Other group communications middleware products include RTCast (University of Michigan), Cactus (University of Arizona), and Spread (Johns Hopkins University).

No standards or commercially produced products exist for group communications. The group communications products that are currently obtainable are generally open-source, experimental products developed by university researchers and maintained by dedicated developers, researchers, and/or users.

However, this class of middleware products is very important to building systems that provide seamless fault tolerance via application replication. The alternative to using a group communications middleware product is to build this essential but complex functionality into every state data-critical interface of a replicated application. Not only is this process labor intensive, but it is prone to introducing defects into the application code as well. Thus, there is ample motivation to solve this specialized problem for the real-time community.

OMG is working to address this situation within the CORBA community. The OMG Fault Tolerant CORBA specification defines a fault tolerance capability that works in conjunction with the CORBA distributed object standard. This specification clearly states that group communications middleware is required as an underlying communications protocol if state-consistency of replicated objects is to be achieved. Recently, OMG has issued a Request for Proposals (RFP) for the development of a reliable, ordered, multicast communication protocol standard. Although this standard, when complete, will not likely fully replace a group-ordered communications middleware, it will provide much of the critical functionality in a way that allows interoperability between implementations.

In view of the importance of this class of middleware in building reliable real-time systems that are fault tolerant and scalable, effort should be invested in ensuring that this capability is available for use in the design and development of OACE. This may be accomplished via one or more of the following approaches.

a. Work within the OMG community to encourage group-ordered communication standardization within the CORBA envelope.

b. Develop an alternative strategy such as a higher-level framework providing group-ordered communication functionality on top of another middleware protocol class (e.g., CORBA or publish-subscribe).

c. Develop or adapt a Navy middleware solution that incorporates group-ordered communication functionality.

These three alternatives are listed in order of preference. Least preferred is the last one, the development of a custom solution for Navy use. However, this class of protocol is sufficiently important to justify selection of the third alternative if neither of the first two approaches proves to be viable.

4.8.5 Data Parallel

This class of distribution middleware is used primarily in parallel processing applications, such as signal processing. Products of this class are primarily intended for communication across the backplane of a massively parallel processor, although many products allow for communication across a network. Two standards exist, including Message Passing Interface (MPI) and Message Passing Interface-Real-Time (MPI-RT). Of these, MPI is clearly the most widely used.

Many implementations of MPI are available, including multiple open-source products and commercially obtainable products. MPI-RT is not as mature as MPI and does not have a significant number of implementations. Also, a substantial niche of researchers in the parallel processing domain uses a data parallel software package, Parallel Virtual Machine (PVM), which is not compliant with either the MPI or MPI-RT standards.

The OMG has recently adopted a specification for Data Parallel CORBA, which is undergoing finalization. This specification is based on the most commonly used features of MPI. Implementations of Data Parallel CORBA are expected to be available in 2004.

4.9 FRAMEWORKS

A framework is a reusable, tailorable design in the form of code for all or part of a software system. For example, a user interface framework provides a design and code for the user interface of a system. A framework generally is an object-oriented design. It doesn't have to be implemented in an object-oriented language, though it usually is. Large-scale reuse of object-oriented libraries requires frameworks. The framework provides a context for the components in the library to be reused.

A framework middleware is a software implementation that provides some generic functionality to other applications through some means of instantiation or definition of application specific data and/or processing. Currently framework middleware technology support for mission-critical and real-time applications is very limited. Examples of framework capabilities include event handling, scheduling, concurrency, and container support. Additionally, some languages (e.g., C++ and Java) supply libraries that provide very rudimentary capabilities, such as containers and graphics interface support.

The current state of the practice in DoD is for contractors to develop framework middleware specifically targeted to a given tactical system's requirements and configuration. Framework products to support required capabilities of an OACE (i.e., fault tolerance, RM, and security) are not currently available. No standards for frameworks exist. In the future, OA may participate in the development of a set of framework standards.

4.10 INFORMATION MANAGEMENT

Information management services facilitate sharing persistent data/objects across applications. Information management services to manage the life cycle of data/objects include creation, reading, updating and deletion (CRUD). Data management services that manage the concurrent access to data/objects by multiple applications include transaction management, locking, versioning, and checkpointing. Collectively, these services are referred to as a database management system (DBMS).

There are currently three published DBMS standards supported by existing commercial and open-source products that are applicable to the OACE: the ISO SQL Object/Relational DBMS standards family and the Java Community Process JDO and JDBC standards.

Early versions of SQL concerned only relational DBMSs with data organized into two-dimensional tables with rows of attributes of standard data types. SQL has evolved to include object-oriented capabilities such as user-defined data types with object behavior provided by user-defined methods bound to those data types.

SQL also provides bindings to a large selection of programming languages and extensions that cover a wide variety of application areas.

JDO grew out of work started by the Object Database Management Group (ODMG) Java language binding. The ODMG standard addressed both C++ and Java bindings, but wide industry acceptance and consistent implementations of the C++ bindings was not achieved for the C++ binding. The ODMG decided to cease work on the C++ binding and transfer its work on the Java binding to the Java Community process where it was the starting point for the JDO standard.

JDO provides persistence of Java objects to either object-oriented or SQL-based datastores via an identical application program interface. JDO's transparent persistence mechanism (where persistent and transient objects are consistently manipulated with standard Java language constructs rather than using SQL for persistent objects and Java for transient objects) can reduce the complexity and code size for applications requiring object-oriented access to legacy relational databases. JDO is therefore complementary to SQL but limited to OA applications utilizing the Java programming language/environment.

JDBC provides a widely accepted standard interface to relational databases from the Java programming language/environment. JDBC may be preferable to JDO for OA applications that have less complicated data models than may warrant JDO or are leveraging COTS products, (i.e, application servers) that utilize JDBC.

4.11 RESOURCE MANAGEMENT (RM)

Distributed Computing RM utilizes RM mechanisms to assign resources to applications depending upon the situation that the tactical platform finds itself in. For example, as new Anti-Air Warfare (AAW) threats are identified, the pool of processors may increase the resources provided to meet these threats. Later when the situation changes, this same pool of processors can adapt to meet another increased threat (e.g., an Anti-Surface Warfare (ASW) threat). This allows a flexible approach responsive to changing tactical situation and resource failures versus the current stovepipe approach where a fixed inflexible set of hardware and infrastructure software is preallocated to a specific tactical application.

The RM technology products can be separated into two distinct categories: static RM and dynamic RM. Static RM provides for the manual and/or predefined startup, shutdown, allocation, and reallocation of software processes. Dynamic RM provides for the automatic startup, shutdown, allocation, and reallocation of software processes based on some detected change (i.e., policy, performance, failure, etc.) in the system.

At present, there are no standards defined for either static or dynamic RM technologies. There are several standards organizations working on business-oriented RM-related standards, many of which are potentially applicable for niche areas within the scope of OA RM. However, there are currently no encompassing RM standards. Standards bodies currently involved with RM-related standards include World Wide Web Consortium (W3C), Distributed Management Task Force (DMTF), and the Internet Engineering Task Force (IETF).

As examples, eXtensible Markup Language (XML), Common Information Model (CIM), and Simple Network Management Protocol (SNMP) are potentially applicable within various RM sub-areas. In addition, there is ongoing work in the Java community, primarily the Java 2 Enterprise Edition (J2EE) , on standards for web and business application monitoring, fault recovery, and scalability; the applicability of these efforts will need to be periodically reassessed.

While there may be instances where static RM products may be useful in an OA system, the more desirable products would be those that fit into the category of dynamic RM. It is well to note that any dynamic RM product will likely have the ability to be used as a static RM product if needed.

A dynamic RM product appropriate for an OA system should contain most, if not all, of the following features:

a. Application/process instrumentation

b. Operating system instrumentation

c. Network instrumentation

d. System health monitoring

e. Resource and application control

f. System and resource specifications (including structure, capabilities, and requirements)

g. Fault detection/fault isolation/fault recovery

h. Dynamic resource allocation

The technology of dynamic RM is in its infancy. As mentioned previously, there is no single product that is both mature and complete in its coverage of the functions required for Navy real-time systems. To further development in this area, the Naval Surface Warfare Center Dahlgren Division (NSWCDD) has begun development on a dynamic RM prototype. This prototype is being used to demonstrate this technology and to encourage maturing the concepts of RM into industry products and future standards. Efforts within the Open Group and the OMG are starting to look at this area.

4.12 SECURITY SERVICES

In order to be consistent with commercial industry's current state of practice, the OA security services are provided using a configuration of "system-high" enclaves of processors that use accredited guard technologies (e.g., Radiant Mercury) to communicate between enclaves at different security levels. It is an OA goal to ensure that the OA application software is unaware of the security mechanisms used at lower layers to protect data and computing resources. Also, the current state of technology does not support a fully multilevel security (MLS) architecture without using proprietary, non-accredited, vendor-specific products. OA will be actively monitoring the progress of the MLS efforts and will be opportunistic in using such capabilities where needed (e.g., coalition warfare) as such capabilities obtain OA validation and DoD Information Technology (IT) Security Certification and Accreditation Process (DITSCAP) accreditation.

For the purposes of the OACE, technologies that provide the infrastructure’s security services have been placed in one of two broad categories: commercial best practice or data separation. The state of industry standards for the technology in each of these categories varies, with a substantial number of technologies having no industry standards.

4.12.1 DoD Policy Constraints

The selection of standards for each of the technologies is constrained by DoD policy. All DoD-owned or controlled information systems that receive, process, store, display or transmit DoD information (regardless of mission assurance category, classification, or sensitivity) must adhere to DoD Directive 8500.1 [reference i].

DoD Directive 8500.1 "establishes policy and assigns responsibilities … to achieve DoD Information Assurance (IA) through a defense-in-depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network centric warfare." DoD Directive 8500.1 does not currently apply to weapons systems, but it does currently apply to the interconnection of a weapons system to an external network.

4.12.2 Commercial Best Practice

Commercial best practice information security technologies are those that commercial industry has pursued and deployed to protect commercial assets. Examples of commercial best practice technology include firewalls, anti-virus software packages, and Intrusion Detection Systems (IDSs). No industry standards are available for commercial best practice products. It is anticipated that OA guidance will be provided in the future for selecting commercial best practice products.

4.12.3 Data Separation

Data separation technologies provide a method to separate data with differing classification levels. Examples of data separation technologies include IP security, encryption algorithms implemented in hardware and/or software, and hardened or trusted operating systems. No comprehensive set of standards exists that fully covers the data separation category. For example, there are no industry standards for a trusted operating system. However, there are a number of standards for cryptographic algorithms that are mandated by the OACE.

The classification level of the information to be protected will dictate the standard to be used. For classified information, it is DoD policy to acquire and use devices that implement Type 1 encryption. The vendors that provide these components are approved and certified by the National Security Agency. No standards are available for Type 1 encryption algorithms.

4.13 TIME SYNCHRONIZATION

Time synchronization for OACE is provided in accordance with a Common Time Reference Architecture. The requirement is to synchronize all time sources to Coordinated Universal Time (United States Naval Observatory) (UTC [USNO]). OACE assumes the existence of a Common Time Reference that is synchronized to UTC (USNO) presumably via the Global Positioning System (GPS) with disciplined oscillators. The Network Time Protocol (NTP) and Inter-Range Instrumentation Group (IRIG) are the time standards used for the distribution and synchronization of time information within the platform. Three initial categories of products have been identified in the time synchronization area: NTP Servers, NTP Client Software, and IRIG Time Interfaces.

4.14 PROGRAMMING LANGUAGES

While numerous higher-level programming languages exist in industry and academia today, OA has selected two to provide the basis for all new development: Java and C++.

Java, developed by Sun Microsystems, has become so pervasive as to qualify as a *de facto* open standard. The Java standards evolve through the Java Community Process where membership is open to anyone, but the characteristics of the language are defined in the reference identified in Section 0 below. In order to legally qualify as Java (the *Java* trademark is owned by Sun), a vendor's product must conform to Sun's specification of the language, as well as to the Sun Java Virtual Machine (JVM).

C++, originally created by Bjarne Stroustrup and now defined in the C++ standard identified in Section 0 below, added object-oriented programming features to the powerful and popular C programming language, of which it is a superset (therefore, C++ compilers are capable of compiling C programs). While early C++ compilers often left much to be desired in terms of speed of the generated executable, modern compilers are capable of producing code whose performance rivals that from C compilers.

Ada 95 is included in Section 0 below to support recent legacy use of software developed in Ada.

SECTION 5

STANDARDS AND OACE COMPLIANCE STATEMENTS

It is the intention of the Navy that all OACE products be standards-based to the maximum extent possible. This document provides the computing standards required by OA.

A primary source for the OACE standards has been the JTA. The current version of the JTA (Version 6.0) is intended to be the last version released. In the future, standards will be listed on-line in the DoD Information Technology Standards and Profiles Registry (DISR). The initial standards listed by the DISR have come from JTA Version 6.0. OA personnel are participating in working groups of the Information Technology Standards Committee (ITSC) who will be maintaining the DISR. For this version of the OACE Technologies and Standards document, the JTA (Version 6.0) is referenced since at this time the DISR is still being stood up. Future OACE Standards documents will utilize the DISR as a primary reference.

To the maximum extent possible, the OACE standards will be mandated by the JTA (currently) or the DISR (in the future). In any case where a mandated JTA or DISR standard is inadequate for OACE, OA personnel will work within the appropriate ITSC working group(s) to resolve the issue. Such situations are therefore anticipated to be temporary conditions which once resolved, the OACE standards and the DISR will be in accord. Additionally, it is expected that the ITSC and OA will each mandate standards that are outside the scope of the other. For example, JTA version 6.0 mandates standards not in the scope of OA, and this document identifies technologies and standards outside the scope of JTA version 6.0 (e.g., dynamic RM and physical media). OA identifies three types of standards: Mandatory, Emerging, and Guidance. The designations ***Mandatory*** and ***Emerging*** are derived from the JTA and have the same meaning in defining the status of OACE standards as these designations do in the JTA. These two designations are defined in JTA, Version 6.0, Volume 1, Section 1.9, which states:

> *"The mandatory standards in the JTA must be implemented or used by systems that have a need for the corresponding JTA service/interface. A standard is mandatory in the sense that if a service/interface is going to be implemented, it shall be implemented in accordance with the associated standard. If a required service/interface can be obtained by implementing more than one standard (e.g., operating system standards), the appropriate standard should be selected based on system requirements."*

And in JTA, Version 6.0, Volume 1, Section 1.7.1:

> *"Emerging Standards … an information-only description of standards that are candidates for possible additions to the JTA mandated standards. … The purpose of listing these candidates is to help the program manager determine those areas likely to change within three years and to suggest those areas in which "upgradability" should be a concern. The expectation is that emerging standards will be elevated to "mandatory" status when implementations of the standards*

> *mature. Emerging standards may be implemented, but shall not be used in lieu of a mandated standard."*

Standards with an OACE status of ***Guidance*** provide information that should be followed. Taking an approach different than that described within a referenced document with an OACE status of ***Guidance*** does not affect the OACE compliance of system, application, or infrastructure. It is recommended that such exceptions be clearly documented during the system's or component's development.

The OACE compliance statements provided below are directed towards the following tactical developers:

a. Infrastructure Component Suppliers

b. Platform Infrastructure Integrators

c. Tactical Software Developers

Table 5-1 provides a listing of the OACE technology areas that have a compliance statement and those currently without a compliance statement. Only the technology areas that have a compliance statement are considered in assessing whether a system has met OACE compliance.

Table 5-1. Technology Area OACE Compliance

COMPLIANCE STATEMENTS	*NO COMPLIANCE STATEMENTS*
Physical Media	Enclosures
Information Transfer	Computing Resources
Operating Systems	Peripherals
Distribution Middleware	Adaptive Middleware
Information Management	Frameworks
Security Services	Resource Management
Time Synchronization	
Programming Languages	

The OACE is providing a common infrastructure for Naval warfighting system development. For this reason, it is critical not to use capabilities (whether from standards, products, or services) not specified in this document that fall within a Technology Area with a compliance statement.

Within the compliance statements below, "**shall**" statements must be met, and "**should**" statements must be met or rationale provided for an exception. The rationale needs to include the impact this exception will have on application software developed above the OACE infrastructure.

The standards provided at this time comprise the core of the OACE standards. A change management process is being put in place for further developing the OACE Standards Set.

5.1 PHYSICAL MEDIA

Shipboard fiber optic system design shall be in accordance with the Fiber Optic System Design Criteria Standard MIL-STD-2052 listed below.

The Fiber Optic Cable Topology (FOCT) should be developed and designed using the *Fiber Optic Shipboard Cable Topology Design Guidance*, MIL-HDBK-2051, listed in Table 5-2. Physical Media Standards.

The FOCT shall be installed and tested in accordance with the *Fiber Optic Cable Topology Installation Standard Methods For Naval Ships*, MIL-STD-2042, listed in Table 5-2. Physical Media Standards.

All fiber optic physical media products/components used shall be in accordance with the OA physical media specifications listed in Table 5-2. Physical Media Standards and those products/components listed in the *Navy Recommended Fiber Optic Components Parts List* dated 21 May 2003 [reference j] or later. All other physical media products/components shall be in accordance with the OA physical media specifications listed in Table 5-2. Physical Media Standards.

All military or commercial fiber optic single terminus connectors used for equipment connections shall be housed within the equipment or an interconnection box.

Copper cable shields shall be grounded by approved 360-degree grounding connectors at terminating equipment and enclosures, connection or junction boxes and at points of penetration into topside areas.

Table 5-2. Physical Media Standards

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Fiber Optic System Design						
Fiber Optic System Design	Shipboard Fiber Optic System Design Requirements	MIL-STD-2052	Mandatory	NAVSEA	Published	No
Fiber Optic Topology Design Guidance						
Fiber Optic Shipboard Cable Topology Design Guidance	Shipboard Cable Plant Design	MIL-HDBK-2051	Guidance	NAVSEA	Published	No
Fiber Optic Topology Installation and Test Standards						
Fiber Optic Cable Topology Installation Standard Methods for Naval Ships	Shipboard Fiber Optic Installation Methods	MIL-STD-2042	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods for Naval Ships (Cables)	Shipboard Fiber Optic Cable Installation Methods	MIL-STD-2042-1	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods for Naval Ships (Equipment)	Shipboard Fiber Optic Equipment Installation Methods	MIL-STD-2042-2	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods for Naval Ships (Cable Penetrations)	Shipboard Fiber Optic Penetration Installation Methods	MIL-STD-2042-3	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods for Naval Ships (Cableways)	Shipboard Fiber Optic Cableway Installation Methods	MIL-STD-2042-4	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods for Naval Ships (Connectors and Interconnections)	Shipboard Fiber Optic Connector Installation Methods	MIL-STD-2042-5	Mandatory	NAVSEA	Published	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Fiber Optic Cable Topology Installation Standard Methods for Naval Ships (Tests)	Shipboard Fiber Optic Installation Tests	MIL-STD-2042-6	Mandatory	NAVSEA	Published	No
Fiber Optic Cable Topology Installation Standard Methods for Naval Ships (Pierside Connectivity Cable Assemblies and Interconnection Hardware)	Fiber Optic Pierside Connectivity Installation Methods	MIL-STD-2042-7	Mandatory	NAVSEA	Published	No
Optical Fiber						
Fiber, Optical, Type I, Class I, Size IV, Composition A, Wavelength B, Radiation Hardened (Metric)	Multimode 62.5 Micron Optical Fiber	MIL-PRF-49291/6	Mandatory	DoD	Published	No
Fiber. Optical, Type II, Class 5, Size II, Composition A, Wavelength D, Radiation Hardened (Metric)	Singlemode Optical Fiber	MIL-PRF-49291/7	Mandatory	DoD	Published	No
Optical Fiber Cable						
Cable, Fiber Optic, Eight Fibers, Enhanced Performance, Cable Configuration Type 2 (OFCC), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard 8-Fiber Cable	MIL-PRF-85045/17	Mandatory	DoD	Published	No
Cable, Fiber Optic, Four Fibers, Enhanced Performance, Cable Configuration Type 2 (OFCC), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard 4-Fiber Cable	MIL-PRF-85045/18	Mandatory	DoD	Published	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Cable, Fiber Optic, Twenty Four, Thirty Three, and Thirty Six Fibers, Enhanced Performance, Cable Configuration Type 2 (OFCC), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard 36-Fiber Cable	MIL-PRF-85045/20	Mandatory	DoD	Published	No
Cable, Fiber Optic, Seven Tube, Blown Optical Fiber, Standard and Enhanced Performance, Cable Configuration Type 5 (Tube), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard 7-Tube BOF Cable	MIL-PRF-85045/25	Mandatory	DoD	Published	No
Cable, Fiber Optic, One Tube, Blown Optical Fiber, Standard and Enhanced Performance, Cable Configuration Type 5 (Tube), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard Single-Tube BOF Cable	MIL-PRF-85045/26	Mandatory	DoD	Published	No
Cable, Fiber Optic, Six-Fiber Bundle, Blown Optical Fiber, Cable Configuration Type 1 (Buffered Fiber), Application B (Shipboard), Cable Class SM And MM, (Metric)	Shipboard 6-Fiber BOF Bundle	MIL-PRF-85045/27	Mandatory	DoD	Published	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Cable, Fiber Optic, Nineteen Tube, Blown Optical Fiber, Standard and Enhanced Performance, Cable Configuration Type 5 (Tube), Application B (Shipboard), Cable Class SM and MM, (Metric)	Shipboard - Tube BOF Cable	MIL-PRF-85045/28	Emerging	DoD	Draft	No
Single Terminus Connectors						
Connector, Fiber Optic, Single Terminus, Plug, Adapter Style, 2.5 Millimeters Bayonet Coupling, Epoxy	Shipboard Light Duty ST Single-Fiber Connector	MIL-C-83522/16	Mandatory	DoD	Published	No
Connector, Fiber Optic, Single Terminus, Adapter, Bayonet Coupling (ST Style), 2.5 Millimeter Diameter Ferrule, Bulkhead Panel Mount	Shipboard Light Duty ST Single-Fiber Connector Adapter	MIL-C-83522/17	Mandatory	DoD	Published	No
Commercial Intermateability Standards						
Fiber Optic Connector Intermateability Standard	COTS ST Dimensional Standard	TIA/EIA-604-2	Mandatory	Telecommunications Industry Association	Published	No
Fiber Optic Connector Intermateability Standard Type SC	COTS SC Dimensional Standard	TIA/EIA-604-3	Mandatory	Telecommunications Industry Association	Published	No
Fiber Optic Connector Intermateability Standard	COTS LC Dimensional Standard	TIA/EIA-604-10	Mandatory	Telecommunications Industry Association	Published	No
Multi Terminus, Heavy Duty Connectors						
Connectors, Fiber Optic, Circular, Plug and Receptacle Style, Multiple Removable Termini, General Specification For	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Connectors	MIL-PRF-28876	Mandatory	DoD	Published	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Connectors, Fiber Optic, Circular, Receptacle Style, Multiple Removable Termini, Screw Threads, Wall Mounting, Without Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Receptacle Connectors	MIL-PRF-28876/1	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug Style, Multiple Removable Termini, Screw Threads, Without Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Cable Plug Connectors	MIL-PRF-28876/6	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug Style, Multiple Removable Termini, Screw Threads, With Straight Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Cable Plug Connectors	MIL-PRF-28876/7	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug Style, Multiple Removable Termini, Screw Threads, With 45 Deg. Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Cable Plug Connectors	MIL-PRF-28876/8	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug Style, Multiple Removable Termini, Screw Threads, With 90 Deg. Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Cable Plug Connectors	MIL-PRF-28876/9	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug Style, Multiple Removable Termini, Dust Cover, Screw Threads, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Cable Plug Dust Cover	MIL-PRF-28876/10	Mandatory	DoD	Published	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Connectors, Fiber Optic, Circular, Receptacle Style, Multiple Removable Termini, Screw Threads, Jamnut Mounting, Without Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Receptacle Connectors	MIL-PRF-28876/11	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Receptacle Style, Multiple Removable Termini, Dust Cover, Screw Threads, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Receptacle Dust Cover	MIL-PRF-28876/15	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug and Receptacle Style, Multiple Removable Termini, Screw Threads, Straight Backshell, Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Connector Backshells	MIL-PRF-28876/27	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug and Receptacle Style, Multiple Removable Termini, 45 Deg. Backshell, Screw Threads, With Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Connector Backshells	MIL-PRF-28876/28	Mandatory	DoD	Published	No
Connectors, Fiber Optic, Circular, Plug and Receptacle Style, Multiple Removable Termini, 90 Deg. Backshell, Screw Threads, With Strain Relief, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Connector Backshells	MIL-PRF-28876/29	Mandatory	DoD	Published	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Connectors, Fiber Optic, Circular, Receptacle Style, Multiple Removable Termini, Screw Threads, Light Duty Backshell, Environment Resisting	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Receptacle Backshells	MIL-PRF-28876/30	Emerging	DoD	Draft	No
Connectors, Fiber Optic, Circular, Receptacle Style, Multiple Removable Termini, Screw Threads, EMI Retention Nut	Shipboard Heavy Duty Multifiber Fiber Optic Equipment Receptacle EMI Backshell	MIL-PRF-28876/31	Emerging	DoD	Draft	No
Optical Fiber Termini						
Termini, Fiber Optic, Connector, Removable, Environment Resisting, Class 5, Type II, Style A, Pin Terminus, Size 16, Rear Release, MIL-C-38999, Series I, III, and IV	Pin Termini for MIL-C-38999 Series I, III, and IV Connectors	MIL-T-29504/4B	Mandatory	DoD	Published	No
Termini, Fiber Optic, Connector, Removable, Environmental Resisting, Class 5, Type II, Style A, Socket Terminus, Size 16, Rear Release MIL-C-38999, Series I, III, and IV	Socket Termini for MIL-C-38999 Series I, III, and IV Connectors	MIL-T-29504/5B	Mandatory	DoD	Published	No
Termini, Fiber Optic, Connector, Removable, Environment Resisting, Class 5, Type II, Style A, Pin Terminus, Front Release, Ceramic Guide Bushing	Pin Termini for MIL-PRF-28876 Connectors	MIL-PRF-29504/14	Mandatory	DoD	Published	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Termini, Fiber Optic, Connector, Removable, Environment Resisting, Class 5, Type II, Style A, Socket Terminus, Front Release, Ceramic Guide Bushing	Socket Termini for MIL-PRF-28876 Connectors	MIL-PRF-29504/15	Mandatory	DoD	Published	No
Boxes						
Interconnection Box, Fiber Optic, Metric, General Specification for	Shipboard Fiber Optic Interconnection Boxes	MIL-I-24728	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Submersible, 354 x 330 MM	One-Module Shipboard Fiber Optic Interconnection Box	MIL-I-24728/1	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Submersible, 308.4 X 609.6 MM	Two-Module Shipboard Fiber Optic Interconnection Box	MIL-I-24728/2	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Submersible, 406.4 X 863.6 MM	Three-Module Shipboard Fiber Optic Interconnection Box	MIL-I-24728/3	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Submersible, 101.6 X 177.8 MM	Small Shipboard Fiber Optic Interconnection Box	MIL-I-24728/4	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Submersible, 152.4 X 228.6 MM	Small Shipboard Fiber Optic Interconnection Box	MIL-I-24728/5	Mandatory	DoD	Published	No
Interconnection Box, Fiber Optic, Connector Patch Panel Module	ST Patch Panel for Shipboard One, Two, and Three Module Fiber Optic Interconnection Boxes	MIL-I-24728/6	Mandatory	DoD	Published	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Enclosures for Electrical Fittings and Fixtures	General Purpose Tube Routing Boxes for BOF Cables	MIL-E-24142	Mandatory	DoD	Published	No
Blown Optical Fiber Components						
Plug, Tube Fitting, Blown Optical Fiber	Tube Fitting Plugs for BOF Tube Fittings	A-A-59728	Mandatory	DoD	Published	No
Furcation Units, Tube, Blown Optical Fiber	Furcation Units for BOF Tubes	A-A-59729	Mandatory	DoD	Published	No
Plugs, Tapered Tube, Blown Optical Fiber	Tube Plugs for BOF Tubes	A-A-59730	Mandatory	DoD	Published	No
Tube Fittings, Blown Optical Fiber	Tube Fittings/ Connectors for BOF Tubes	A-A-59731	Mandatory	DoD	Published	No
Copper Cable Topology Installation and Test Standards						
Electrical Plant Installation Standard Methods for Surface Ship and Submarines	Shipboard Copper Cable Installation Methods	DOD-STD-2003	Mandatory	DoD	Published	No
Shipboard Electrical/Electronic/ Fiber Optic Cable; Remove, Relocate, Repair, And Install	Shipboard Installation and Test for Copper/Fiber Optic Cable	NAVSEA Standard Item Number 009-73	Mandatory	NAVSEA	Published	No
Commercial Building Telecommunications Cabling Standard, Part 2: Balanced Twisted Pair Cabling Components	Installation Testing For Category 5E Electrical Connectors/ Cable	TIA/EIA-568B.2	Mandatory	Telecommunications Industry Association	Published	No
Copper Cable, Twisted Pair						
Cables, Light-Weight, Electric, Low Smoke, For Shipboard Use, General Specification For	General Specification for Shipboard Copper/ Electrical Cable	MIL-C-24640	Mandatory	NAVSEA	Published	No
Cables and Cords, Electric, Low Smoke, for Shipboard Use, General Specification for	General Specification for Shipboard Copper/ Electrical Cable	MIL-C-24643	Mandatory	NAVSEA	Published	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Cable, Electrical, Type LSC5OS	Shipboard Category 5E Twisted Pair Cable	MIL-C-24643/59	Emerging	NAVSEA	Draft	No
Cable, Electrical, Local Area Network	Light Duty Commercial Category 5E Twisted Pair Cable	A-A-XXXXX	Emerging	NAVSEA	Draft	No
Connectors, Twisted Pair						
Connectors, Electrical, Circular, Screw Threads, High Shock, High Density, Crimp Contacts Receptacle, Jam Mounting, Class D and DS	Heavy Duty Shipboard Circular Electrical Connector	MIL-C-28840/14	Mandatory	DoD	Published	No
Connectors, Electrical, Circular, Screw Threads, High Density, High Shock, Shipboard, Crimp Contacts Plug, Class D and DS	Heavy Duty Shipboard Circular Electrical Connector Plug	MIL-C-28840/16	Mandatory	DoD	Published	No
Commercial Building Telecommunications Cabling Standard, Part 2: Balanced Twisted Pair Cabling Components	Light Duty Commercial RJ-45 Category 5E Electrical Connectors	TIA/EIA-568B.2	Mandatory	Telecommunications Industry Association	Published	No

5.2 ENCLOSURES

No OA standards are identified at this time for Enclosures. However, OA guidance suggests that the industry standard 19"-wide rack mounting be utilized for installing COTS equipment aboard naval platforms. COTS products to be mounted in enclosures include computers, peripherals and network switches. There are no vertical spacing requirements or recommendations provided at this time.

5.3 INFORMATION TRANSFER

All OACE components will require an information transfer capability. An information transfer capability is composed of numerous subcomponents, depending on the functionality required. Functionality choices include connectivity type (e.g., Gigabit Ethernet), basic and specialized transfers (e.g., Stream Control Transmission Protocol [SCTP]), and support services required (e.g., File Transfer Protocol [FTP] and telnet). Each subcomponent capability shall be implemented in accordance with the applicable standards listed below. As a result, an individual instance of OACE will include a selected subset of the standards listed below based on the sub-component capabilities chosen.

NOTE: DoD has issued a directive regarding migration to Internet Protocol Version 6 (IPv6). Some of the base specifications for IPv6 are included as emerging systems in the table below. Later editions of this document will more fully address the use of IPv6 in OACE-based systems.

Table 5-3. Information Transfer Standards

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Connectivity (Lower Layer) Protocols						
Fast Ethernet	100 Mbps half and full duplex over twisted pairs and optical fiber cables	IEEE Std 802.3-2002	Mandatory	IEEE 802	Standard	Yes, Vol I, 3.6.1(a), See Note 1
Gigabit Ethernet	1,000 Mbps full duplex over twisted pairs and optical fiber cables	IEEE Std 802.3-2002	Mandatory	IEEE 802	Standard	Yes, Vol I 3.6.6(a), See Note 1

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
10 Gigabit Ethernet	10,000 Mbps full duplex over optical fiber cables	IEEE 802.3ae-2002	Emerging	IEEE 802	Standard	No
Aggregation of Multiple Link Segments	Provides for increased link availability and bandwidth by providing mechanisms for parallel link segment aggregation.	IEEE Std 802.3-2002	Mandatory	IEEE 802	Standard	No
Power Over Ethernet	DTE power via MDI	IEEE 802.3af-2003	Mandatory	IEEE 802	Standard	No
Media Access Control (MAC) Bridges	MAC Bridging, includes Spanning Tree Algorithm and Protocol	IEEE Std 802.1D, 1998 Edition (with amendment IEEE 802.1t-2001)	Mandatory	IEEE 802	Standard	No
Traffic Class Expediting and Dynamic Multicast Filtering	This supplement, incorporated into IEEE 802.1D, 1998 Edition, defines additional capabilities for traffic class expediting and dynamic multicast address filtering.	IEEE Std 802.1D, 1998 Edition	Mandatory	IEEE 802	Standard	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Virtual Bridged Local Area Networks	Defines the operation of Virtual LAN (VLAN) Bridges that permit the definition, operation and administration of VLAN topologies within a Bridged LAN infrastructure.	IEEE 802.1Q-2003	Mandatory	IEEE 802	Standard	Yes, Vol II 3.5.4.1(a), See Note 1
Port-Based Network Access Control	A supplement to IEEE Std 802.1D, 1998 Edition. Defines the changes necessary to the operation of a MAC Bridge in order to provide Port based network access control capability.	IEEE 802.1X-2001	Emerging	IEEE 802	Standard	No
Rapid Reconfiguration	A supplement to IEEE Std 802.1D, 1998 Edition. Defines the changes necessary to the operation of a MAC Bridge in order to provide rapid reconfiguration capability.	IEEE 802.1w-2001	Emerging	IEEE 802	Standard	No
802.11b, WiFi	Wireless LANs in 2.4 GHz band	IEEE 802.11b-1999	Emerging	IEEE 802	Standard	Yes, Vol II, 3.6.1(a)
802.11a	Wireless LANs in newly allocated UNII, 5 GHz, band	IEEE 802.11a-1999	Emerging	IEEE 802	Standard	Yes, Vol II, 3.6.1(a)

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
802.11g	Wireless LANs with higher speed(s) PHY extension to the IEEE 802.11b standard	IEEE 802.11g	Emerging	IEEE 802	Standard	No
802.11i	Enhance the 802.11 MAC to enhance security and authentication mechanisms	IEEE 802.11i	Emerging	IEEE 802	Standard	No
Bluetooth	Wireless Personal Area Networks	IEEE 802.15.1-2002 (Bluetooth v1.1)	Emerging	IEEE 802 and Bluetooth Special Interest Group (SIG)	Standard	No
RPR	Resilient Packet Ring	IEEE 802.17	Emerging	IEEE 802	Standard	No
Fibre Channel	High performance serial link supporting its own, as well as other, protocols at various speeds.	ANSI X3.230-1994 / AM 2-1996	Mandatory	ANSI, Fibre Channel Industry Association (FCIA)	Standard	Yes, Vol I, C4ISR.5.2.1.1(a)
SCSI	Small Computer System Interconnect, multiple versions	Numerous standards (including ANSI x3.131)	Mandatory	ANSI / NCITS T10	Standard	Yes, Vol I, WS.GV.4.3.2.2(a), WS.MS.5.1.2.2(a), Vol I, WS.MUS.4.2.1.1(a)
USB	Universal Serial Bus, multiple versions	USB 2.0	Mandatory	USB Implementers Forum	Standard	No
Firewire	High-performance serial bus communications	IEEE 1394-1995	Emerging	IEEE	Standard	Yes, Vol I, C4ISR. 5.2.1.2(a), WS.SS.4.2.1 (a)

Standard Title	Purpose	Standard ID	OACE Status	Standards Organization	Standards Status	In JTA?
InfiniBand	Channel-based, switched fabric, interconnect architecture for servers	InfiniBand 1.1	Emerging	InfiniBand Trade Association	Standard	No
Transfer (Middle Layer) Protocols						
IP, also IPv4	Internet Protocol, version 4	RFCs 791, 950, 919, 922, 1112, (STD 5)	Mandatory	IETF	Standard	Yes Vol I, 3.4.1.11(a), 3.5.2(a)
ICMP	Internet Control Message Protocol	RFCs 792, 950 (STD 5)	Mandatory	IETF	Standard	Yes, Vol I, 3.4.1.11(a), 3.5.2(a)
ARP	Address Resolution Protocol	RFC 826 (STD 37)	Mandatory	IETF	Standard	Yes, Vol I, 3.6.1(a)
IGMPv3	Internet Group Management Protocol, version 3	RFC 3376	Mandatory	IETF	Proposed Standard	Yes, Vol I, 3.4.1.11(a), 3.5.2(a), See Note 1
IP over Ethernet	Transmission of IP Datagrams over Ethernet Networks	RFC 894 (STD 41)	Mandatory	IETF	Standard	Yes, Vol I, 3.6.1(a)
RIPv2	Routing Information Protocol, version 2	RFC 2453 (STD 56)	Mandatory	IETF	Standard	No
TCP	Transmission Control Protocol	RFCs 793, 3168 (STD 7)	Mandatory	IETF	Standard	Yes, Vol I, 3.4.1.10.1(a) , 3.5.1(a)
UDP	User Datagram Protocol	RFC 768 (STD 6)	Mandatory	IETF	Standard	Yes, Vol I, 3.4.1.10.2(a) , 3.5.1(a)
OSPFv2	Open Shortest Path First, version 2	RFC 2328 (STD 54)	Mandatory	IETF	Standard	Yes, Vol I, 3.5.3.1(a)
BGP4	Border Gateway Protocol, version 4	RFCs 1771, 1772	Mandatory	IETF	Draft Standard	Yes, Vol I, 3.5.3.2(a)

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
PPP	Point to Point Protocol	RFCs 1661, 1662 (STD 51)	Mandatory	IETF	Standard	Yes, Vol I, 3.6.2(a)
VRRP	Virtual Router Redundancy Protocol	RFC 2338	Emerging	IETF	Proposed Standard	No
MPLS	Multi-Protocol Label Switching	RFC 3031	Emerging	IETF	Proposed Standard	Yes, Vol II, 3.5.4.1(a)
DVMRP	Distance Vector Multicast Routing Protocol	RFC 1075	Emerging	IETF	Experimental	No
PIM - Sparse Mode	Protocol Independent Multicast - Sparse Mode	RFC 2362	Emerging	IETF	Experimental	No
RTP	Transport Protocol for Real-Time Applications	RFC 3550	Emerging	IETF	Draft Standard	Yes, Vol II, 3.4.1.13(a)
RARP	Reverse ARP	RFC 907 (STD 40)	Mandatory	IETF	Standard	No
IPv6	Internet Protocol, version 6	RFC 2460	Emerging	IETF	Draft Standard	Yes, Vol I, 3.4.1.11(a), 3.5.2(a)
ICMPv6	ICMP, version 6	RFC 2463	Emerging	IETF	Draft Standard	Yes, Vol I, 3.4.1.11(a), 3.5.2(a)
ND for IPv6	Neighbor Discovery for IPv6 (IPv6)	RFC 2461	Emerging	IETF	Draft Standard	Yes, Vol I, 3.4.1.11(a), 3.5.2(a)
IPv6 Autoconfiguration	IPv6 Stateless Address Autoconfig-uration	RFC 2462	Emerging	IETF	Draft Standard	Yes, Vol I, 3.4.1.11(a), 3.5.2(a)
Addressing Architecture	IPv6 Addressing Architecture	RFC 3513	Emerging	IETF	Draft Standard	Yes, Vol II, 3.4.1.11(a)

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Address Format	An IPv6 Global Unicast Address Format	RFC 3587	Emerging	IETF	Informational	Yes, Vol II, 3.4.1.11(a)
Support (Upper Layer) Protocols						
DHCP	Dynamic Host Configuration Protocol	RFC 2131	Mandatory	IETF	Draft Standard	Yes, Vol I, 3.4.1.7(a), 3.5.1(a)
FTP	File Transfer Protocol	RFC 959 (STD 9)	Mandatory	IETF	Standard	Yes, Vol I, 3.4.1.3(a)
Telnet	Remote Terminal Protocol	RFCs 854, 855	Mandatory	IETF	Standard	Yes, Vol I, 3.4.1.4(a)
SMTP	Simple Mail Transport Protocol	RFCs 2821, 1870	Mandatory	IETF	Standard	Yes, Vol I, 3.4.1.1(a)
RSVP	Resource Reservation Protocol	RFCs 2205, 2750	Emerging	IETF	Proposed Standard	Yes, Vol II, 3.4.1.12(a), 3.5.4.1(a)
DNS	Domain Name System	RFCs 1034, 1035, 2136 (STD 13)	Mandatory	IETF	Standard	Yes, Vol I, 3.4.1.2.3(a)
SIP	Session Initiation Protocol	RFCs 3261, 3262, 3263, 3264, 3265	Emerging	IETF	Proposed Standard	Yes, Vol II, 3.4.1.13(a)
H.323	Packet-based Multimedia Communications Systems, version 2	ITU-T Recommendation H.323	Emerging	ITU		Yes, Vol II, 3.4.1.13(a)
Megaco	Gateway Control Protocol, version 1	RFC 3525	Emerging	IETF	Proposed Standard	Yes, Vol II, 3.4.1.13(a)
SNMP	Simple Network Management Protocol	RFC 1157 (STD 15)	Mandatory	IETF	Historic	Yes, Vol I, 3.8.1(a)
RMON	Remote Network Monitoring MIB, version 1	RFC 2819	Mandatory	IETF	Standard	Yes, Vol I, 3.8.1(a)

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
RMON2	Remote Network Monitoring MIB, version 2	RFC 2021	Mandatory	IETF	Proposed Standard	Yes, Vol II, 3.8.1(a)
HTTPv1.1	Hypertext Transfer Protocol, version 1.1	RFCs 2616, 2817	Mandatory	IETF	Draft Standard	Yes, Vol I, 3.4.1.8.1(a)
LDAPv3	Lightweight Directory Access Protocol, version 3	RFCs 2251, 3377	Mandatory	IETF	Proposed Standard	Yes, Vol I, 3.4.1.2.2(a), See Note 1
RADIUS	Remote Authentication Dial-In User Service	RFCs 2865, 3575	Emerging	IETF	Draft Standard	Yes, Vol II, 6.4.1.3.2(a), See Note 1
SSHv2	Secure Shell, version 2	See Note 2.	Emerging	IETF		Yes, Vol II,. 6.4.1.5(a), CS.DTS.5.2(a)
BOOTP	Bootstrap Protocol	RFCs 951, 2132, 1542	Mandatory	IETF	Draft Standard	Yes, Vol I, 3.4.1.6(a)
TFTPv2	Trivial File Transfer Protocol, version 2	RFCs 1350, 2347, 2348, 2349 (STD 33)	Mandatory	IETF	Standard	Yes, Vol I, 3.5.1(a)
DiffServ	Differentiated classes of service for Internet traffic	RFCs 2474, 3168	Emerging	IETF	Proposed Standard	Yes, Vol II, 3.5.4.1(a)
SCTP	Stream Control Transmission Protocol	RFCs 2960, 3309	Emerging	IETF	Proposed Standard	No
FCIP	Fibre Channel over TCP/IP	IETF Draft	Emerging	IETF		No
iSCSI	Internet SCSI. Protocol to carry SCSI over IP networks	IETF Draft	Emerging	IETF		No

Standard Title	Purpose	Standard ID	OACE Status	Standards Organization	Standards Status	In JTA?
NFSv4	Network File System, version 4	RFC 3530	Emerging	IETF	Proposed Standard	No
NNTP	Network News Transfer Protocol	RFC 977	Mandatory	IETF	Proposed Standard	No
SNMPv3	Simple Network Management Protocol, version 3	RFCs 3411-3418 (STD 62)	Emerging	IETF	Standard	Yes, Vol II, 3.8.1(a), See Note 1
MIB-II	Management Information Base for TCP/IP-based internets, MIB-II	RFC 1213 (STD 17)	Mandatory	IETF	Standard	Yes, Vol I, 3.8.1(a)
OSPFv2 MIB	MIB for OSPFv2	RFC 1850	Mandatory	IETF	Draft Standard	Yes, Vol I, 3.8.1(a)
MIB	MIB for Ethernet-like interfaces	RFC 1643 (STD 50)	Mandatory	IETF	Standard	Yes, Vol I, 3.8.1(a)
Note 1: JTA 6.0 references older version of standard or document.						
Note 2: SSHv2 is a de facto industry standard used extensively. The IETF is in the process of standardizing SSH. The current drafts are: draft-ietf-secsh-architecture-15.txt, draft-ietf-secsh-transport-17.txt, draft-ietf-secsh-connect-18.txt dated October 2003.						

5.4 COMPUTING RESOURCES

No OA standards are identified at this time for Computing Resources. However, OA guidance suggests that OA systems be constructed using pools of commercially available commodity processors (e.g., PC-based) able to perform server and/or client processing.

5.5 OPERATING SYSTEMS

Operating System compliance is based on implementing and using the key APIs from IEEE 1003.1-2003. When **real-time** capabilities (as defined by IEEE 1003.13) are required, compliance is based on implementing and using the mandatory features of IEEE 1003.13–2003 Profile 54. This profile selects features specified within IEEE 1003.1 and IEEE 1003.26. Conformance tests are now available for IEEE 1003.1-2003, when a sufficient number of conformant products are available, it is OA's plan to replace the compliance requirement with a conformance requirement (when **real-time** capabilities are required to include the mandatory features of IEEE 1003.13 Profile 54).

Profile 54 defined by the IEEE 1003.13-2003 standard was selected for the OA operating system standard because it is appropriate for large, complex real-time applications needing a wide variety of functionality from their operating systems. However, it should be noted that the differences between Profile 53 and Profile 54 are currently being studied in detail for use by OA Compliant applications, and it is possible that this requirement will be changed to Profile 53 in a future update. The primary capabilities provided by Profile 54 that are not available in Profile 53 are those needed for multiple independent, non-cooperating, interactive users, such as time-sharing systems; Profile 53 assumes that one or more applications are running under control of a single user or several cooperating users. It is critical to note that the requirement for any specific profile is oriented toward the OA Compliant applications, not the operating system. This means that the application must be designed to use only operating system interfaces and capabilities defined by the selected profile. Because each IEEE 1003.13-2003 profile is a proper subset of the higher profiles, an OA application can be executed on any operating system compliant with the selected profile or higher, if any. For example, if Profile 53 is selected for application program development, any operating system compliant with either Profile 53 or Profile 54 can be used.

The OA operating system standards provide for implementations that utilize either general purpose or real-time operating systems. Below are the OA operating system standards:

a. For the OACE Compliant categories, an operating system selected to be used on individual processors or throughout a pool of processors shall be compliant with IEEE 1003.1-2003 [reference f] *Standard*. OACE mandatory capabilities shall include the POSIX mandatory core facilities and all the facilities that provide:

1. POSIX Parent/Child Relationship Multiple Processing model [e.g., multiple POSIX processes, fork () and exec ()]
2. POSIX Signals
3. POSIX Threads
4. POSIX Timers
5. POSIX Message Queues
6. POSIX Semaphores
7. POSIX Shared Memory

b. For the Fully OACE Compliant categories, an operating system selected for use for individual processors or throughout a pool of processors to support real-time application requirements shall comply to the mandatory features of Profile 54 of IEEE 1003.13–2003 [reference g], as applied to IEEE 1003.1-2003. In assessing OACE compliance for a particular system, application program or infrastructure, if that compliance is based on using this real-time functionality, it shall be called out within any assessment of their OACE compliance (e.g., a system is OACE Standards (Category 3) category, Version 1 compliant using the real-time functionality).

c. While the operating system industry is presently developing POSIX 1003.1-2003 conforming products, there are not sufficient numbers of available products for OA to mandate this version of POSIX 1003.1. For this reason, OACE compliance currently can be met via using an operating system compliant to the previous versions of this standard (IEEE 1003.1-1996 and IEEE 1003.2-1993) that includes the OACE mandatory capabilities listed above. For each ***pool of processors*** implemented (or used), all processors shall use the same POSIX base (either POSIX 1003.1-2003 or the earlier IEEE 1003.1-1996 and IEEE 1003.2-1993. In assessing OACE compliance for a particular system, application program or infrastructure, if that compliance is based on using the earlier IEEE 1003.1-1996 and IEEE 1003.2-1993, the exact version shall be called out within any assessment of their OACE compliance (e.g., a system is OACE Standards (Category 3) category, Version 1 compliant using the IEEE 1003.1-1996 and IEEE 1003.2-1993 real-time functionality). No special assessment qualification is required for a particular system, application program or infrastructure that utilizes POSIX 1003.1-2003. It is the intent of OA to remove this option in the future as the operating system industry matures its POSIX 1003.1-2003 capabilities.

d. For the Fully OACE Compliant categories, the operating system selected should follow the guidance provided within IEEE 1003.0-1995, *IEEE Guide to the POSIX Open System Environment (OSE).*

e. For the Fully OACE Compliant categories, operating system component suppliers providing additional features (i.e., APIs) beyond those of IEEE 1003.1–2003 (as described above) and/or POSIX 1003.13-2003 Profile 54 (for real-time usage**)** needed to utilize their products (e.g., in I/O control and devices) shall be described in open (i.e., distribution unlimited) documentation.

f. For the Fully OACE Compliant categories, operating system users (e.g., middleware and application developers) shall utilize the capabilities standardized by IEEE 1003.1–2003 as described above wherever possible. Real-time operating system users shall utilize the mandatory items of POSIX 1003.13-2003 Profile 54 wherever possible. Where additional functionality is needed (e.g., in I/O control and devices), all instances of additional functionality shall be identified within the documentation developed (e.g., flagged within the source code) to support future reuse/porting of the software. Inappropriate usage of such additional functionality (e.g., using proprietary APIs where POSIX functionality is available) may result in the OACE noncompliance of the application program.

g. While the preferred OACE operating system compliance approach is via the POSIX standards listed within this section, a second alternative is currently acceptable as the Linux community develops true POSIX capabilities. OA shall accept the use of the standard Linux equivalent functionality (e.g., Linux threads vs. POSIX threads, Linux signals vs. POSIX signals) in place of the POSIX functionality. .It is recommended that applications choosing to use Linux select a distribution that is compliant to the Linux Standard Base (LSB), defined by the Free Standards Group. The functionality provided by the selected Linux distribution shall include the Linux equivalent functionality for the OACE mandatory capabilities listed above. For each ***pool of processors*** implemented (or used), all processors shall use the same functionality (either the POSIX or the Linux functionality). In assessing OACE compliance for a particular system, application program or infrastructure, if that compliance is based on using the equivalent Linux functionality, it shall be called out within any assessment of their OACE compliance (e.g., a system is OACE Standards (Category 3) category, Version 1 compliant using the Linux operating system real-time functionality). No special assessment qualification is required for a particular system, application program or infrastructure that utilizes POSIX-compliant functionality. It is the intent of OA to remove this option in the future as the Linux community matures its POSIX capabilities.

Table 5-4. Operating System Standards

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Base Definitions, IEEE 1003.1 Standard for Information Technology - Portable Operating System Interface (POSIX)	Mandated Services	IEEE 1003.1 - 2003	Mandatory	IEEE	Standard	No
System Interfaces, IEEE 1003.1 Standard for Information Technology - Portable Operating System Interface (POSIX)	Mandated Services	IEEE 1003.1 - 2003	Mandatory	IEEE	Standard	No
Shells and Utilities, IEEE 1003.1 Standard for Information Technology - Portable Operating System Interface (POSIX)	Mandated Services	IEEE 1003.1 - 2003	Mandatory	IEEE	Standard	No
Rationale (informative), IEEE 1003.1 Standard for Information Technology - Portable Operating System Interface (POSIX)	Guidance	IEEE 1003.1 - 2003	Guidance	IEEE	Standard	No
IEEE Guide to the POSIX Open System Environment (OSE)	Guidance	IEEE 1003.0 - 1995	Guidance	IEEE	Standard	No
IEEE Standard for Information Technology - Standardized Application Environment Profile - POSIX® Realtime Application Support	Environment Profiles	IEEE 1003.13 - 2003	Mandatory	IEEE	Standard	Yes Vol II 2.5.7 (references ISO/IEC equivalent) (See Note 1)

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
IEEE Guide for Developing User Open System Environment (OSE) Profiles	Guidance	IEEE 1003.23-1998	Guidance	IEEE	Approved Publication of IEEE	No
Portable Operating System Interface (POSIX) - Part 26: Device Control Application Program Interface (API) [C Language]	Mandated Services	IEEE 1003.26-2003	Emerging	IEEE	Emerging Std	No
Linux Standards Base	Binary System Interface Specification	Linux Standard Base 2.0	Guidance	Free Standards Group (www.linuxbase.org)	Current Version	Yes Vol I 2.5.7 (See Note 1)
IEEE 1003.1-1996: Information Technology — Portable Operating System Interface (POSIX) — Part 1: System Application Program Interface (API) [C Language] Incorporating IEEE 1003.1-1990, 1003.1b-1993, 1003.1c-1995, and 1003.1i-1995	Mandated Services	IEEE 1003.1-1996	Mandatory (temporary optional alternative to IEEE Std 1003.1 - 2003)	IEEE & ISO/IEC	Standard	Yes Vol I 2.5.7
IEEE 1003.2: Information Technology — Portable Operating System Interface (POSIX) — Part 2: Shell and Utilities	Mandated Services	IEEE 1003.1-1993	Mandatory (temporary optional alternative to IEEE Std 1003.1 - 2003)	IEEE & ISO/IEC	Standard	Yes Vol I 2.5.7
IEEE 1003.1-2003 is an update to IEEE 1003.1-2001 that incorporates Technical Corrigenda 1-2002, and Technical Corrigenda 2-2003.						
Note 1: JTA 6.0 references older versions of standard or document.						

5.6 PERIPHERALS

No specific OA peripherals standards are identified at this time.

5.7 ADAPTIVE MIDDLEWARE

No specific OA standards are identified at this time for adaptive middleware. However, OA guidance suggests that adaptive middleware products selected for use should be based on the POSIX family of operating system standards. In addition, it is preferable that the product allow for wide usage across many different operating systems and computing resources platforms.

5.8 DISTRIBUTION MIDDLEWARE

Four types of distribution middleware are identified for OA usage: distributed objects, publish-subscribe protocols, group-ordered communication protocols and message-passing middleware for data parallel applications. At this time, only the distributed objects and the message-passing middleware for data parallel applications have mature standards to identify. An interim approach is provided for the publish-subscribe functionality.

For the Fully OACE Compliant categories, the distribution middleware selected to support application requirements shall meet the requirements provided in the following subsections. All application program message transfer shall be provided by the Distribution Middleware capabilities described below and not by the direct access of capabilities provided by other technology areas (e.g., operating system sockets). Each of the following subsections covers a different functionality; only those functionalities required by a system needs to be implemented/used.

5.8.1 Distributed Objects

For the Fully OACE Compliant categories or the OACE Interface category, if distributed objects middleware is needed, the following are required for OACE compliance:

a. The application shall use CORBA distributed objects middleware to meet all distributed objects middleware requirements other than interfaces to legacy systems.

b. The application shall use a CORBA product that conforms to the standards specified.

c. The application shall not make use of any proprietary (non-standard) features of the selected product(s).

d. The application shall not make use of any optional CORBA parts of the CORBA standard, standardized CORBA services or facilities that are not specifically listed below.

5.8.2 Publish-Subscribe

For the Fully OACE Compliant and the OACE Interface categories, if publish-subscribe middleware is needed, the middleware product selected shall be compliant with the Platform Specific Model (PSM) of the OMG Data Distribution Service (DDS) standard’s minimal profile. Prior to January 1, 2006, publish-subscribe middleware used shall be based on a current product offering that the middleware vendor is committed to upgrade, by January 1, 2006, to an implementation compliant with the DDS standard’s minimal profile.

The Data Distribution Service (DDS) specification [reference h] has been finalized by the OMG who will formally publish the DDS standard in 2004. The finalized specification includes both a Platform Independent Model (PIM) and a single PSM. The PIM defines the capabilities and semantics provided by the specification whereas a PSM defines the mapping of those capabilities and semantics to the syntax of a particular execution environment. Although in the future there may be multiple PSMs for the DDS, only one PSM is currently defined within the DDS specification. That PSM is based on CORBA Interface Design Language (IDL). The use of CORBA IDL allows for DDS implementations in all languages for which there exists a CORBA IDL language mapping, including Java, C++, C, and Ada. While the DDS specification does not require the PSM; as previously stated, OA requires application developers to limit DDS usage to the interfaces defined by the PSM. Portability between DDS implementations can be attained only if a common PSM is utilized.

The DDS specification identifies multiple compliance profiles, including the minimum profile, content-subscription profile, persistence profile, ownership profile, and object model profile. At this point in time, it is unclear if there will be multiple vendors supporting each of these profiles. Thus, distribution middleware users (e.g., application developers) shall not rely on features from any profile other than the minimum profile. It is the intent of OA to consider the use of additional DDS profiles in the future if a need for the additional functionality is found and these additional profiles are supported in the products of multiple vendors.

At this point in time, DDS specification based middleware products provided by different vendors are not anticipated to be interoperable. Thus coordination in the fielding of DDS based middleware products across an OACE compliant infrastructure is needed. It is the intent of OA to participate in the DDS standards work to enable DDS based communications between products from multiple vendors.

In stating OACE compliance for a particular system or product, if publish-subscribe middleware is required, the product selected shall be called out within any assessment of their OACE compliance (e.g., a system is OA Common Functions [Category 4] category, Version 1 compliant using the DDS [place vendor/product names/version number here] publish-subscribe middleware).

5.8.3 Group-Ordered Communications

There are no standards or products selected for group-ordered communications distribution middleware. This technology is deemed to be too immature for use in operational systems. As group-ordered communications products and standards are developed, this situation may change and OA may provide standards for use.

5.8.4 Message-Passing Interface for Data Parallel Applications

If a data parallel application requires message-passing interfaces, the following are required for OACE compliance:

a. The application shall use middleware product(s) that are MPI/MPI-RT compliant, to the standards listed below, to meet all message passing for data parallelism middleware requirements other than interfaces to legacy systems.

b. The application shall not make use of any proprietary (non-standard) features of the selected product.

It is the intent of OA to move towards the CORBA data parallel standards as the OMG matures these capabilities and commercial products become available.

Table 5-5. Distribution Middleware Standards

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Distributed Objects						
Common Object Request Broker Architecture (CORBA v2.6)	Interface Repository - chapter 10	formal/02-06-33	Mandatory	OMG	Standard	Yes Vol I 2.5.11.1 See Note 1
Common Object Request Broker Architecture (CORBA v2.6)	CORBA Interoperability - chapter 12	formal/02-06-33	Mandatory	OMG	Standard	Yes Vol I 2.5.11.1 See Note 1
Common Object Request Broker Architecture (CORBA v2.6)	General Inter-ORB Protocol - chapter 15	formal/02-06-33	Mandatory	OMG	Standard	Yes Vol I 2.5.11.1 See Note 1
Common Object Request Broker Architecture (CORBA v2.6)	Portable Interceptors - chapter 21	formal/02-06-33	Mandatory	OMG	Standard	Yes Vol I, 2.5.11.1 See Note 1
Common Object Request Broker Architecture (CORBA v2.6)	Messaging - chapter 22	formal/02-06-33	Mandatory	OMG	Standard	Yes Vol I, 2.5.11.1 See Note 1
Common Object Request Broker Architecture (CORBA v2.6)	Fault Tolerant CORBA - chapter 23	formal/02-06-33	Mandatory	OMG	Standard	Yes Vol I, 2.5.11.1 See Note 1
Common Object Request Broker Architecture (CORBA v2.6)	Common Secure Interoperability-chapter 24	formal/02-06-33	Mandatory	OMG	Standard	Yes Vol I, 2.5.11.1 See Note 1
Real-Time CORBA Static Scheduling Spec v1.1	Real-time CORBA	formal/02-08-02	Mandatory	OMG	Standard	No
Minimum CORBA Spec v1.0	Minimum CORBA	formal/02-08-01	Mandatory	OMG	Standard	No
CORBA Data Parallel Spec	CORBA Data Parallel Spec	pending formalization	Emerging	OMG	pending formalization	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Real-Time CORBA Dynamic Scheduling Spec 2.0	Real-Time CORBA Dynamic Scheduling	pending formalization	Emerging	OMG	pending formalization	No
CORBA Extensible Transports	CORBA Extensible Transports	pending formalization	Emerging	OMG	pending formalization	No
CORBA Unreliable Multicast Spec v1.0	CORBA Unreliable Multicast	pending formalization	Emerging	OMG	pending formalization	No
CORBA Reliable Ordered Multicast	CORBA Reliable Ordered Multicast	in progress	Emerging	OMG	in progress	No
CORBA Services						
Life-cycle Services Spec v2	Life-cycle Services	formal/02-09-01	Mandatory	OMG	Standard	No
Naming Service Spec, v2	Naming Service	formal/02-09-01	Mandatory	OMG	Standard	Yes Vol I, 2.5.11.1(a), See Note 1
Notification Service Spec, v1.0.1, Aug 2002	Notification Service	formal/02-08-04	Mandatory	OMG	Standard	Yes Vol I, 2.5.11.1(a), See Note 1
Security Services Spec v1.7, Mar 2001	Secure Distributed Services	formal/02-03-08	Emerging	OMG	Standard	No
Persistent State Service Spec, v2.0, Aug 1999	Persistent State Service	formal/02-09-06	Mandatory	OMG	Standard	No
CORBA Component Model v3.0, Jun 2002	CORBA Component Model	formal/02-06-65	Mandatory	OMG	Standard	No
CORBA FTAM/FTP Interworking Spec, v1.0, March 2002	CORBA FTAM/FTP Interworking	formal/02-03-13	Mandatory	OMG	Standard	No
CORBA Concurrency Service v1.0, Apr 2000	CORBA Concurrency Service	formal/00-06-14	Mandatory	OMG	Standard	No
Time Service Spec v1.1, May 2002	Time Service	formal/02-05-06	Mandatory	OMG	Standard	Yes Vol I, 2.5.11.1(a), See Note 1
Enhanced View of Time Spec, v1.1, May 2002	Time Service	formal/02-05-07	Mandatory	OMG	Standard	No

Standard Title	Purpose	Standard ID	OACE Status	Standards Organization	Standards Status	In JTA?
Event Service Spec, v1.1, March 2001	Event Service	formal/01-03-01	Mandatory	OMG	Standard	Yes Vol I, 2.5.11.1(a), See Note 1
Externalization Service Spec, v1.0, May 2000	Externalization Service	formal/00-06-16	Mandatory	OMG	Standard	No
Transaction Service Spec, v1.4, Sep 2003	Transaction Service	formal/03-09-03	Mandatory	OMG	Standard	Yes Vol I, 2.5.11.1(a), See Note 1
Trading Object Service Spec, v1.0, June 2000	Trading Object Service	formal/00-06-27	Mandatory	OMG	Standard	Yes Vol I
Publish Subscribe						
Data Distribution Specification for Real-Time Systems	Data Distribution	in progress	Mandatory Starting 1/1/2006	OMG	In Progress	No
Group Ordered Comms						
NONE						
Message Passing for Data Parallel Apps						
Extensions to the Message Passing Interface, July 1997	Message Passing Interface	MPI-2	Mandatory		Standard	No
CORBA Data Parallel Spec	CORBA Data Parallel Spec	Pending Formalization	Emerging	OMG	Pending Formalization	No
Other Message-Oriented Middleware						
Extensible Markup Language (XML) 6 October 2000	XML	XML 1.0 (Second Edition)	Mandatory	W3C	Standard	Yes Vol I, 2.5.4.1(a)
Note 1: JTA 6.0 references older versions of standard or document.						

5.9 FRAMEWORKS

No specific OA standards are identified at this time for Frameworks.

5.10 INFORMATION MANAGEMENT

OA compliance in the area of information management consists of:

a. Implementers shall use the SQL family of standards and/or the JDO or JDBC standards for the management of persistent data/objects as listed below.

b. The SQL family of standards cited below covers a wide range of capabilities. Implementers shall select a subset of the standards cited below that have wide industry acceptance and consistent implementations suitable for their applications.

c. The use of the Java-related portions of the SQL family of standards and the JDO and JDBC standards, all cited below, is limited to those OA applications utilizing Java.

Table 5-6. Information Management Standard

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
SQL						
Structured Query Language (SQL)	Part 1: Framework (SQL/ Framework)	ISO/IEC 9075-1:1999	Mandatory	ISO	Standard	Yes (emerging) Vol II, 2.5.3(a)
Structured Query Language (SQL)	On-Line Analytical Processing (SQL/OLAP)	ISO/IEC 9075-1:1999/Amd 1:2001	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	Part 2: Foundation (SQL/Foundation)	ISO/IEC 9075-2:1999	Mandatory	ISO	Standard	Yes (emerging) Vol II, 2.5.3(a)
Structured Query Language (SQL)	On-Line Analytical Processing (SQL/OLAP)	ISO/IEC 9075-2:1999/Amd 1:2001	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	Part 3: Call-Level Interface (SQL/CLI)	ISO/IEC 9075-3:1999	Mandatory	ISO	Standard	Yes (emerging) Vol II, 2.5.3(a)
Structured Query Language (SQL)	Part 4: Persistent Stored Modules (SQL/PSM)	ISO/IEC 9075-4:1999	Mandatory	ISO	Standard	Yes (emerging) Vol II, 2.5.3(a)

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Structured Query Language (SQL)	Part 5: Host Language Bindings (SQL/Bindings)	ISO/IEC 9075-5:1999	Mandatory	ISO	Standard	Yes (emerg-ing) Vol II, 2.5.3(a)
Structured Query Language (SQL)	On-Line Analytical Processing (SQL/OLAP)	ISO/IEC 9075-5:1999/Amd 1:2001	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	Part 9: Management of External Data (SQL/MED)	ISO/IEC 9075-9:2001	Mandatory	ISO	Standard	Yes (emerg-ing) Vol II, 2.5.3(a)
Structured Query Language (SQL)	Part 10: Object Language Bindings (SQL/OLB)	ISO/IEC 9075-10:2000	Mandatory	ISO	Standard	Yes (emerg-ing) Vol II, 2.5.3(a)
Structured Query Language (SQL)	Part 13: SQL Routines and Types Using the Java TM Programming Language (SQL/JRT)	ISO/IEC 9075-13:2002	Mandatory (Applicable if Java is used)	ISO	Standard	No
Structured Query Language (SQL)	Remote Database Access for SQL With Security Enhancement	ISO/IEC 9579:2000	Mandatory	ISO	Standard	Yes (emerg-ing) Vol II, 2.5.3(a)
Structured Query Language (SQL)	SQL Multimedia and Application Packages – Part 1: Framework	ISO/IEC 13249-1:2002	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	SQL Multimedia and Application Packages – Part 2: Full-Text	ISO/IEC 13249-2:2000	Mandatory	ISO	Standard	No
Structured Query Language (SQL)	SQL Multimedia and Application Packages – Part 3: Spatial	ISO/IEC 13249-3:1999	Mandatory	ISO	Standard	Yes (emerg-ing) Vol II, 2.5.3(a)
Structured Query Language (SQL)	SQL Multimedia and Application Packages – Part 5: Still Image	ISO/IEC 13249-5:2001	Mandatory	ISO	Standard	No

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Structured Query Language (SQL)	SQL Multimedia and Application Packages – Part 6: Data Mining	ISO/IEC 13249-6:2002	Mandatory	ISO	Standard	No
JDO/JDBC						
Java Data Objects (JDO)	Java Object Persistence to Object Oriented or Object/Relational Data Stores	Version 1.0:3/25/2002	Mandatory (Applicable if Java is used)	Java Community Process	Standard	No
JDBC 3.0 Specification	Java object Persistence to Object/Relational Data Stores	Version: 3.0, December 1, 2001	Mandatory (Applicable if Java is used)	Java Community Process	Standard	Allowed (Not Mandated) Vol I, 2.5.3(a)

5.11 RESOURCE MANAGEMENT

No OA standards are identified at this time for Resource Management.

5.12 SECURITY SERVICES

All OA systems will need to address security services and determine the security services to be implemented (e.g., authentication and encryption). If a specific security service (e.g., authentication) is required and there is a standard for that service in the following list, that security service shall be implemented in accordance with the applicable standards listed below. Additionally:

a. All DoD-owned or controlled information systems, other than weapon systems, that receive, process, store, display or transmit DoD information, regardless of mission assurance category, classification or sensitivity shall adhere to DoD Directive 8500.1 [reference i].

b. Any conflict in OACE security standards with DoD Directive 8500.1 will be resolved by following the policy of Directive 8500.1.

c. If security service technology requires an evaluation, all evaluations shall follow the Common Criteria process.

Table 5-7. Security Services Standards

Standard Title	Purpose	Standard ID	OACE Status	Standards Organization	Standards Status	In JTA?
Generic						
The Common Criteria, version 2.1	Common Criteria to Evaluate the Security of IT Systems	ISO/IEC 15408	Mandatory	ISO	Standard	Yes Vol I, 6.8.1
Kerberos Network Authentication	Provides Access Control and Authentication Mechanisms for Network Devices	RFC 1510	Mandatory	IETF	Proposed Standard	Yes Vol I, 6.4.1.3.2 (a)
GSS-API	Provides a Programming Interface for Various Security Services	RFC 2743	Mandatory	IETF	Proposed Standard	Yes (emerging) Vol II, 6.4.2.5(b)
RADIUS	Access Control for Remote Users (e.g., Port Authentication)	RFC 2865	Mandatory	IETF	Draft Standard	Yes Vol II, 6.4.1.3.2 (a) Note: JTA calls out older RFC
RADIUS Attributes for Tunnel Protocol Support	To Support Compulsory Tunneling	RFC 2868	Guidance	IETF	Informational	No
IANA Considerations for RADIUS	IANA for RADIUS	RFC 3575	Mandatory	IETF	Proposed Standard	No
Security Architecture for the Internet	Specifies Security Services (Confidentiality, Authentication, Integrity) for IP Packets	RFC 2401	Mandatory	IETF	Proposed Standard	Yes Vol I, 6.6.1(a)
Port Authentication	Authentication Services for Ports on Network Devices	IEEE 802.1x	Mandatory	IEEE	Standard	No
Enhanced Security (for wireless)	Replacement for WEP	IEEE 802.11i	Emerging	IEEE	Draft (not yet released to public)	No

Standard Title	Purpose	Standard ID	OACE Status	Standards Organization	Standards Status	In JTA?
Cryptographic						
Security Requirements for Cryptographic Modules	Cryptographic Modules That Protect Sensitive but Unclassified Data	FIPS 140-2	Mandatory	NIST	Standard	Yes Vol I, 6.4.2.7(a)
Secure Hash Standard	Message Authentication	FIPS 180-1	Mandatory	NIST	Standard	Yes Vol I, 6.4.2.2(a)
Digital Signature Standard		FIPS 186-2	Mandatory	NIST	Standard	Yes Vol II, 6.4.2.1(a)
Advanced Encryption Algorithm	Encryption of Sensitive but Unclassified Data	FIPS 197	Mandatory	NIST	Standard	Yes Vol II, 6.4.2.1(a)
The Keyed Message Authentication Code	Message Authentication	FIPS 198	Mandatory	NIST	Standard	No
The Directory: Authentication Framework	Format for Certificates Containing Public Key Information	ITU-T Rec. X.509 Version 3	Mandatory	ITU	Standard	Yes Vol I, 6.4.1.2(a)
Transport Layer Security	Security Mechanisms (e.g., Confidentiality) for TCP-based Applications	RFC 2246	Mandatory	IETF	Proposed Standard	Yes Vol I, 6.4.1.1(a)
Transport Layer Security Extensions	Extensions to TLS (backwards compatible to RFC 2246)	RFC 3546	Mandatory	IETF	Proposed Standard	No
Internet X.509 PKI Certificate and CRL	Specifies the Use of X.509 Certificates for Use in an Internet Environment	RFC 3280	Mandatory	IETF	Proposed Standard	No
Lightweight Directory Access Protocol Version 3	Specifies the Use of LDAP Services for X.509 Certificates	RFC 3377	Mandatory	IETF	Proposed Standard	No (call out v2, but v2 is obsolete)
IP Authentication Header	Authentication Services for IP Packets	RFC 2402	Mandatory	IETF	Proposed Standard	Yes Vol I, 6.6.1(a)

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
IP Encapsulating Security Payload	Confidentiality Services for IP Packets	RFC 2406	Mandatory	IETF	Proposed Standard	Yes Vol I, 6.6.1(a)
Internet Security Association and Key Management	Key Management Services for IP Packets	RFC 2408	Mandatory	IETF	Proposed Standard	Yes Vol I, 6.6.1(a)

5.13 TIME SYNCHRONIZATION

All OACE components will require time synchronization capability. All OACE components shall provide time synchronization capability using NTP implemented in accordance with the standard listed below. In the event that NTP does not meet mission requirements, an IRIG time synchronization service may be provided and shall be implemented in accordance with the standard listed below.

Table 5-8. Time Distribution Standards

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
Network Time Protocol (NTP) Version 3	Time Synchronization Across a Network	RFC 1305	Mandatory	IETF	Draft Standard	Yes Vol I, 3.4.1.5(a)
IRIG Serial Time Code Formats, Format B (IRIG-B)	Time Synchronization via an I/F Cable	IRIG Standard 200-98, IRIG-B	Mandatory	Range Commander's Council	Standard	Yes C4ISR Vol I, 5.2.2(a)

5.14 PROGRAMMING LANGUAGES

For development of new software in OA:

a. Either Java or C++ shall be used for new software development.

b. Virtual machines used for execution of OA Java applications shall implement the Sun JVM specification listed below, corresponding to that JVM provided in Version 1.4 of the Java Development Kit (JDK), with any deviations from the specification clearly documented and rationales for said deviations provided. JVM vendors shall be required to make all reasonable efforts to maintain compatibility with Sun's JVM for Version 1.4 of the JDK.

c. Java compilers used in OA application development shall be compatible with the Java Language Specification as listed below.

d. If C++ is used, compilers and libraries shall be used that are compatible with the specification listed below.

e. Ada 95 shall not be used for new software development; its use shall be limited to supporting recent legacy applications. When Ada 95 is used, compilers, libraries and associated utilities shall be used that are compatible with the specification listed below.

The Programming Language standards are provided in Table 5-9.

Table 5-9. Programming Language Standards

STANDARD TITLE	PURPOSE	STANDARD ID	OACE STATUS	STANDARDS ORGANIZATION	STANDARDS STATUS	IN JTA?
The Java Virtual Machine Specification, Second Edition	Specification of the Java Virtual Machine (JVM)	Authors: Tim Lindholm, Frank Yellin; Copyright 1997-1999 by Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303	Mandatory	Sun Microsystems (owns Java Trademark)	Standard	No
The Java Language Specification, Second Edition	Specification of the syntax and semantics of the Java programming language	Authors: James Gosling et al.; Copyright 2000 by Sun Microsystems, Inc., 901 San Antonio Road, Palo Alto, CA 94303	Mandatory	Sun Microsystems (owns Java Trademark)	Standard	No
Programming Languages - C++	Specification of the C++ Programming Language	14882:1998	Mandatory	ANSI/ISO/IEC	Standard	No
Information Technology-Programming Languages-Ada	Specification of the Ada 95 Programming Language	8652:1995	Mandatory	ISO/IEC	Standard	No

SECTION 6

OACE COMPLIANCE ASSESSMENT

There are four types of OACE compliance assessments defined. These four types of assessments are covered in the following four subsections. All OACE compliance claims shall clearly identify which type of assessment (of the four) is being made.

A government program manager may make a claim of OACE compliance once that manager believes that all of the requirements for one (or more) of the four compliance assessment types described within this section have been met. A ***Validated Claim*** is one that has the concurrence of the PEO IWS OA Program Office. Validating a claim involves having a neutral party, under the direction of PEO IWS OA Program Office, verifying the specific claim. Validation of OACE assessment claims will be covered by a separate OA document.

6.1 OACE SYSTEM COMPLIANCE ASSESSMENT

The overall goal of the OACE effort is to produce OACE-compliant systems for use aboard Navy platforms. An OACE-compliant system is one where all application programs are fully compliant (as defined within Section 6.2) and whose infrastructures are also fully compliant (as described within Section 6.3). An OACE System may be composed of a number of OACE Infrastructures (computer pools) each of which may have different selections for the technology areas described within Section 5 of this document (e.g., general purpose Linux versus real-time POSIX operating systems).

6.2 OACE APPLICATION PROGRAM COMPLIANCE ASSESSMENT

An OACE-compliant application subsystem is the unit of software that OACE compliance is assessed for and may range from a single small executable (an application program) to a large set of related executables. An OACE compliant application subsystem runs on an OACE Infrastructure (i.e., an individual or a pool of processors) that only requires the capabilities specified within Section 5 of this document for the technology areas that have OACE compliance statements. OACE-compliant application subsystems are required to identify a specific Fully OACE Compliant (Categories 3 or 4) category that they are to run within. Note that the resource requirements of the application program subsystem must be identified in order to determine and configure the pool of computing that it is to run over.

6.3 OACE INFRASTRUCTURE COMPLIANCE ASSESSMENT

An OACE infrastructure is an instantiation of a pool of computing that has been built to run OACE-compliant application programs. An OACE-compliant infrastructure is an instantiation of a pool of computing that meets all of the requirements described within Section 5 of this document AND does NOT use any additional capabilities (whether from standards, products or services) from the technology areas that have OACE compliance statements.

To make a compliance claim, the OACE-defined capabilities must not only exist; they must be configured to operate and perform the functions that they are intended as described in Section 5 of this document. For example, the information transfer routing products usually have a number of routing protocols implemented; however, for the infrastructure to be OACE infrastructure compliant, the OACE-defined functions shall be the only ones actively running (e.g., OSPFv2).

6.4 OACE INTERFACE COMPLIANCE ASSESSMENT

An application that has been ported (or built) using the OACE Interface (Category 2) approach can be claimed as being OACE Interface compliant. This approach specifies an external interface at which point OACE application programs communicate with the Category 2 application program. The Category 2 application program uses an adaptation layer to isolate non-OACE technologies (i.e., middleware, operating systems, etc.) from OACE-compliant application programs. OACE-compliant middleware is used for all communications with OACE-compliant application programs. Legacy distribution middleware (i.e., non-OACE) may be used within the application programs ported using this approach.

To make this compliance claim, an interface instantiation shall be documented that defines the OACE Distribution Middleware standard(s) used (one or more of the OACE middleware standards defined in Section 5.8). The infrastructure on which the Category 2 application runs shall be defined. Any impacts to other OACE technology areas (e.g., Information Management and/or Time Synchronization) shall be defined.

6.5 DOCUMENTING OACE COMPLIANCE ASSESSMENT CLAIMS

A claim shall be written based on the compliance statements in Section 5 of this document. All OACE compliance claims shall clearly identify which type of claim (i.e., system, application program, infrastructure or interface) is being made. All OACE compliance claims referenced against this document shall identify a particular Fully OACE Compliant category (or categories) supported (i.e., Category 3 or 4) or for OACE Interface compliance claim only OACE Interface (Category 2) is applicable. Any OACE compliance assessment claims referenced against this document for a system, application program and/or infrastructure shall specifically identify any exceptions to OACE compliance requirements provided within Section 5 of this document.

An example of a system compliance assessment claim (i.e., for a system with one OACE infrastructure) follows: the XYZ fire control system is OA Common Functions (Category 4) category, OACE Version 1 compliant using the Linux Operating System real-time functionality.

6.6 OACE INFRASTRUCTURE COMPONENTS

For an OACE infrastructure to be fully compliant, it must be built from components (e.g., network routers, computers and operating systems) that implement all of the OACE standards applicable to each component and all components must be configured to use the standards. Such components that are capable of supporting OACE-compliant capabilities are usually also capable of supporting proprietary capabilities. For this reason, components used to build an OACE infrastructure shall neither be described nor claimed to be “OACE compliant” but rather “**fully OACE supportive**.” The key issue is how such components are applied (e.g., configured or coded) to implement a specific infrastructure that determines whether that infrastructure is compliant or not.

APPENDIX A

ACRONYMS

Acronym	**Definition**
AAW	Anti-Air Warfare
ANSI	American National Standards Institute
API	Applications Program Interface
ARP	Address Resolution Protocol
ASN (RDA)	Assistant Secretary of the Navy (Research, Development, and Acquisition)
ASW	Anti-Surface Warfare
BGP	Border Gateway Protocol
BOF	Blown Optical Fiber
BOOTP	Bootstrap Protocol
CD	Compact Disk
CG	Cruiser, Guided Missile
CID	Commercial Item Description
CIM	Common Information Model
CLI	Call-Level Interface
CORBA	Common Object Request Broker Architecture
COTS	Commercial Off-the-Shelf
CRT	Cathode Ray Tube
CRUD	Creation, Reading, Updating, and Deletion
DBMS	Data Base Management System
DCOM	Distributed Component Object Model
DDG	Destroyer, Guided Missile
DDS	Data Distribution Service
DHCP	Dynamic Host Configuration Protocol
DISR	DoD Information Technology Standards and Profiles Registry
DITSCAP	DoD Information Technology Security Certification and Accreditation Process

Acronym	**Definition**
DMTF	Distributed Management Task Force
DNS	Domain Name System
DoD	Department of Defense
DVD	Digital Video Disk
DVMRP	Distance Vector Multicast Routing Protocol
DX/DR	Data Extraction/Data Reduction
EPS	Embedded Processor Subsystem
FOCT	Fiber Optic Cable Technology
FTP	File Transfer Protocol
GPS	Global Positioning System
HM&E	Hull, Mechanical, and Electrical
HTTP	Hyper Text Transfer Protocol
IA	Information Assurance
ICMP	Internet Control Message Protocol
IDL	Interface Design Language
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
I/O	Input/Output
IP	Internet Protocol
IPT	Integrated Product Team
IRIG	Inter-Range Instrumentation Group
ISO	International Standards Organization
IT	Information Technology
IT-21	Information Technology – 21st Century

Acronym	**Definition**
ITSC	Information Technology Standards Committee
J2EE	Java 2 Enterprise Edition
J2SE	Java 2 Standard Edition
JAAS	Java Authentication and Authorization Service
JCP	Java Community Practice
JDBC	Java Database Connectivity
JDO	Java Data Objects
JTA	Joint Technical Architecture
JVM	Java Virtual Machine
LAN	Local Area Network
LCD	Liquid Crystal Display
LCS	Littoral Combat Ship
LDAP	Lightweight Directory Access Protocol
MCE	Mission Critical Enclosure
MDA	Model Driven Architecture
MED	Management of External Data
MIB	Management Information Base
MLS	Multilevel Security
MPI	Message Passing Interface
MPI-RT	Message Passing Interface-Real Time
MPLS	Multi-Protocol Label Switching
MTM	Multipurpose Transportable Middleware
NAS	Network Attached Storage
NAVSEA	Naval Sea Systems Command
ND	Neighbor Discovery
NFS	Network File System

Acronym	**Definition**
NIST	National Institute of Standards and Technology
NNTP	Network News Transfer Protocol
NSWCDD	Naval Surface Warfare Center Dahlgren Division
NTP	Network Time Protocol
OA	Open Architecture
OACE	Open Architecture Computing Environment
ODMG	Object Database Management Group
OLAP	On-Line Analytical Processing
OLB	Object Language Binding
OMG	Object Management Group
ORB	Object Request Broker
OS	Operating System
OSD	Office of the Secretary of the Navy
OSE	Open System Environment
OSI	Open System Interconnection
OSJTF	Open Systems Joint Task Force
OSPF	Open Shortest Path First
PC	Personal Computer
PEO	Program Executive Office
PEO IWS	Program Executive Office for Integrated Warfare Systems
PIM	Platform Independent Model
PIM	Protocol Independent Multicast
PKI	Public Key Infrastructure
POSIX	Portable Operating System Interface Standard
PPP	Point-to-Point Protocol
PSM	Platform Specific Model

Acronym	**Definition**
PSM	Persistent Stored Module
PVM	Parallel Virtual Machine
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RARP	Reverse Address Resolution Protocol
RIP	Routing Information Protocol
RM	Resource Management
RMI	Remote Method Invocation
RPR	Resilient Packet Ring
RSVP	Resource Reservation Protocol
RT	Real Time
RTOS	Real Time Operating System
RTP	Real-time Transport Protocol
SAN	Storage Area Network
SBC	Single Board Computer
SCSI	Small Computer System Interface
SCTP	Stream Control Transmission Protocol
SIG	Special Interest Group
SIP	Session Initiation Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSDS	Ship Self Defense System
TBD	To Be Determined
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol

Acronym	**Definition**
TIA	Telecommunications Industry Association
TP	Twisted Pair
UDP	User Datagram Protocol
UML	Unified Modeling Language
USB	Universal Serial Bus
UTC (USNO)	Coordinated Universal Time according to the United States Naval Observatory
VLAN	Virtual Local Area Network
VME	Virtual Micro-bus European
W3C	World Wide Web Consortium
XML	[E]Xtensible Markup Language